Regulatory Disruption and Arbitrage in Health-Care Data Protection*

Nicolas P. Terry**

Abstract:

This article explains how the structure of U.S. health-care data protection (specifically its sectoral and downstream properties) has led to a chronically uneven policy environment for different types of health-care data. It examines claims for health-care data protection exceptionalism and competing demands such as data liquidity. In conclusion, the article takes the position that health-care-data exceptionalism remains a valid imperative and that even current concerns about data liquidity can be accommodated in an exceptional protective model. However, re-calibrating our protection of health-care data residing outside of the traditional health-care domain is challenging, currently even politically impossible. Notwithstanding, a hybrid model is envisioned with downstream HIPAA model remaining the dominant force within the health-care domain, but being supplemented by targeted upstream and point-of-use protections applying to health-care data in disrupted spaces.

** Hall Render Professor of Law, Executive Director, Hall Center for Law and Health, Indiana University Robert H. McKinney School of Law. Email: npterry@iupui.edu. Frank Pasquale, Kristin Madison, Craig Konnoth were generous with their time in commenting on an early draft. I also thank the workshop participants at the 2015 Amsterdam Privacy Law Scholars Conference (Oct. 2015) and the Health Law Policy, Biotechnology, and Bioethics Workshop at the Petrie-Flom Center at Harvard Law School (Apr. 2016) for their valuable feedback. I also thank the anonymous peer reviewers at the Yale Journal of Health Policy, Law, and Ethics for their helpful comments. Professor Miriam Murphy helped immeasurably with research and Kelci Dye, Indiana University Robert H. McKinney School of Law J.D. candidate, was a diligent editor.

TABLE OF CONTENTS

"Your previous provider refused to share your electronic medical records, but not to worry—I was able to obtain all of your information online."[1]

INTRODUCTION

In 1994, two years before passage of the statute that authorized the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security rules, the Institute of Medicine (IOM) took the position that "legislation should clearly establish that the confidentiality of person-identifiable data is an attribute afforded to the data elements themselves, regardless of who holds the data."[2] That exhortation was ignored, allowing a regulatory vector between the protection of health-care data held inside and outside of the conventional health care space. Policymakers' persistent, systemic failure to safeguard health-care data outside the HIPAA domain is now exemplified by the minimal, sub-HIPAA data protection afforded health-care data either held by data brokers ("companies that collect consumers' personal information and resell or share that information with others"[3]) or created by mobile apps.

The result of this policy misstep is an emerging narrative of regulatory disruption and arbitrage. Simply put, disruption and arbitrage can occur when disruptive businesses in a lightly regulated domain create products previously associated with incumbents of a highly regulated domain.

This is not just another story of emerging technologies exposing the lamentable state of data protection in the United States. It is also an account of the likely depreciation of a health-care-specific policy position that was hard won and as yet has not been convincingly refuted. This policy is health-care privacy exceptionalism. As described below, the fundamental flaw in U.S. data protection was the rejection of generalized or universal protection in favor of a domain-specific model. Virtually alone among those domains, health care carved out a reasonably effective data protection position, referred to as health-care privacy exceptionalism, courtesy of the HIPAA Privacy and Security Rules[4] and their

1. Kaamran Hafeez, *Daily Cartoon*, THE NEW YORKER (Sept. 11, 2015), http://www.newyorker.com/cartoons/daily-cartoon/daily-cartoon-friday-september-11th-healthcare-doctor-visit [https://perma.cc/K3N6-6BW4].

2. INSTITUTE OF MEDICINE, HEALTH DATA IN THE INFORMATION AGE: USE, DISCLOSURE, AND PRIVACY 191 (Molla S. Donaldson & Kathleen N. Lohr eds., 1994) [hereinafter HEALTH DATA IN THE INFORMATION AGE].

3. *Data Brokers: A Call for Transparency and Accountability*, FED. TRADE COMMISSION i (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/M9M5-A6P8] [hereinafter *Data Brokers*].

4. *HIPAA Administrative Simplification, Regulation Text, 45 C.F.R. pts. 160, 162, and 164*

state law analogues.[5] Exceptionalism also has a downside. Conversations about mainstream data protection have tended to ignore, even isolate health care, viewing the domain as *sui generis* and adequately protected by HIPAA.

The key to understanding current disruption and arbitrage in the health-care data sector is an appreciation of the U.S. data protection approach and, obviously, its particular application to health care. While the sectoral nature of U.S. health-care data protections is generally understood, other properties, such as the distinction between upstream and downstream data protection models, may not be so well-known. The intersections of multiple data protection models help explain the current declining state of health-care data protection. Equally, understanding multiple models is helpful in refuting over-simplified binaries (for example, privacy versus data liquidity) and provides insight into potential data protection reforms.

The analysis that follows suggests two examples of regulatory disruption and arbitrage in in health-care data. The first example considers health-care data collected, analyzed, and sold by big data brokers. Some of those data are created within the highly regulated space of health-care practice but legally "exported" (for example, they may have been de-identified). Other big data are created outside the highly regulated health-care domain but are medically inflected, and, once combined with other data points, operate as data proxies for protected HIPAA data. In both scenarios, data triangulation may defeat any de-identification. In the second example, users increasingly generate wellness, fitness, and sickness data on mobile health platforms or by mobile health apps. Again, the picture is complicated (hence the disruption). Some data are created in a highly regulated space but then exported to a mobile device; other data are processed in the opposite direction.

This article takes the position that health-care-data exceptionalism remains a valid imperative and that even current concerns about data liquidity can be accommodated in an exceptional protective model. However, re-calibrating our protection of health-care data residing outside of the traditional health-care domain is challenging. This article envisions a hybrid model, with downstream HIPAA model remaining the dominant force within the health-care domain, supplemented by upstream and point-of-use protections applying to health-care data in disrupted spaces.

(Unofficial Version, as amended through March 26, 2013), U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf [https://perma.cc/P9R8-QH7A].

5. *See generally* Joy L. Pritts, *Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule*, 2 YALE J. HEALTH POL'Y L. & ETHICS 327, 332–40 (2002).

I. BACKGROUND: KEY CHARACTERISTICS OF U.S. DATA PROTECTION

The dysfunctional nature of U.S. data protection is ironic given its often-heralded roots. Samuel Warren and Louis Brandeis's famous Harvard article[6] has achieved mythic fame for birthing its eponymous "Right to Privacy." However, looking back at their article today, it is striking to see the relatively narrow driver that led those famous lawyers to propose the recognition of the "right to be let alone."[7] Primarily, they seemed concerned about some members of the press (perhaps, in today's terms, the paparazzi) and what the authors viewed as an inappropriate appetite for gossip and triviality.[8] Indeed, Jill Lepore has described the article, "a manifesto against the publicity of modernity."[9] Today, the article's "Right to Privacy" title plays better than its substance and, perversely, that title now exists merely as a slogan inaccurately preserving the myth of strong U.S. data protection. Those seeking the source of the contemporary data protection debate are more likely to find it, albeit accompanied by dystopian contexts, in Alan Westin's 1967 book *Privacy and Freedom*[10] or his 1972 preview of today's data broker issues, *Databanks in a Free Society*.[11]

With no little irony given the health-care context of this paper, it was the U.S. Department of Health, Education, and Welfare (HEW), a precursor to the Department of Health & Human Services (HHS), which first considered a comprehensive privacy law applying across all domains and regulating both public and private entities.[12] The HEW report discussed both government and non-governmental information practices[13] and outlined one of the first iterations of Fair Information Practice Principles (FIPPs).[14] FIPPs are a distillation of the best information practices common to developed democracies and, as noted by the Federal Trade Commission (FTC), include some core privacy principles: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress."[15]

---

6. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

7. *Id.* at 195.

8. *Id.* at 196.

9. Jill Lepore, *The Prism: Privacy in an Age of Publicity*, NEW YORKER (June 24, 2013), http://www.newyorker.com/reporting/2013/06/24/130624fa_fact_lepore [https://perma.cc/5AN6-EAH5].

10. ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

11. ALAN F. WESTIN, MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING, AND PRIVACY (1972).

12. SECRETARY'S ADVISORY COMM., U.S. DEP'T. HEALTH, EDUC. & WELFARE, DHEW PUB. NO. (OS) 73–94, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973), http://www.justice.gov/opcl/docs/rec-com-rights.pdf [https://perma.cc/ZU4D-DGC9].

13. *Id.* at 33–46.

14. *Id.* at xx-xxi, xxiii.

15. *Privacy Online: A Report to Congress*, FED. TRADE COMMISSION, 7 (1998),

Unfortunately, the misstep that followed was that the HEW report only recommended, and Congress only enacted, privacy legislation to control the data collecting practices of the federal government. Many of the issues discussed in this article can be traced back to this Pyrrhic victory, the Privacy Act of 1974.[16] What Frank Pasquale has termed U.S. privacy law's "original sin" was the failure to embrace a comprehensive rather than piecemeal approach to data protection.[17]

A. Sectoral Data Protection

Thereafter, as acknowledged by the 2012 White House report, "most Federal data privacy statutes appl[ied] only to specific sectors, such as healthcare, education, communications, and financial services or, in the case of online data collection, to children."[18] The original sin is not just about preferring sectoral to more comprehensive regulation. The patchwork of resulting protections "results from the sectoral approach having been created backwards. Rather than coming up with an overall picture and then breaking it up into smaller pieces that mesh together, Congress has been sporadically creating individual pieces of ad hoc legislation."[19] Thus, the "sectoral approach is emblematic of the lack of a perceptible, cohesive commercial data privacy policy, which creates complexity and costs for businesses and confuses consumers."[20]

The sectoral approach has played out over multiple industries. As is well known, the Gramm–Leach–Bliley Act (GLBA) governs consumer privacy in the financial sector.[21] GLBA, like HIPAA, is sectoral, applying to narrowly defined data custodians, specifically groups of financial entities. Just as HIPAA does not apply to all custodians of health-care data, so GLBA does not apply to all who

---

https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [https://perma.cc/UXR2-VQLC]. The FIPPs are principles or properties of privacy codes that were initially developed by the FTC but are now featured in codes across the world.

16. 5 U.S.C. § 552a (2012).

17. *Episode 7: Mark Rothstein, Big Data & Health Research, Apple ResearchKit, White House Consumer Privacy Bill*, WEEK HEALTH L. (Apr. 8, 2015), http://twihl.podbean.com/e/7-mark-rothstein-big-data-health-research-apple-researchkit-white-house-consumer-privacy-bill/ [https://perma.cc/LQ48-W2RL].

18. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, WHITE HOUSE, 6 (Feb. 2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf [https://perma.cc/4YS7-FWWH] [hereinafter *Framework for Protecting Privacy*].

19. *Commercial Data Privacy and Innovation in the Internet Economy: Dynamic Policy Framework*, U.S. DEP'T COM. 60 (Dec. 2010), http://www.ntia.doc.gov/report/2010/commercial-data-privacy-and-innovation-internet-economy-dynamic-policy-framework [https://perma.cc/PG6Z-V6HM] (summarizing commenters).

20. *Id.* at 59.

21. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 501, 113 Stat. 1338, 1436–37 (1999). *See generally* Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1219–20 (2002).

hold consumer financial data.[22] And like HIPAA, GLBA is a downstream data-protection model that erects a duty of confidentiality[23] and requires notice to consumers of an institution's privacy policies and practices.[24] The Fair Credit Reporting Act (FCRA) applies to consumer reporting agencies regarding important if narrow requirements relating to quality, transparency, and access.[25] Other examples cover still narrower sectors such as video rental records.[26] Even now, with the sectoral approach to data protection understood as causing severe regulatory gaps, calls for narrowly focused "fixes" continue, whether to protect student records from big data brokers[27] or to prevent automobiles from "spying" on their drivers.[28]

A sectoral approach to data protection has other flaws. For example, sectoral models inevitably encourage differential levels of protection, and that more often promotes a race to the bottom rather than to the top. Worse, high levels of protection can be characterized as outliers and targeted for "reform."

This sectoral limitation of substantive law spills over into rulemaking and enforcement. Inter-agency cooperation has never been a core strength of the federal government, and turf wars likely exacerbate regulatory gaps. It is one thing not to have a comprehensive privacy model. It is another not to have a unified data-protection agency. For example, the European Union has had a (relatively) uniform law since 1995.[29] The new General Data Protection Regulation (GDPR)[30] has attracted interest because of its erasure[31] and breach

22. *See* 15 U.S.C. § 6805(a) (2012). Notwithstanding, the FTC does have some broad residual powers. *See* Privacy of Consumer Financial Information; Final Rule, 65 Fed. Reg. 33,646 (May 24, 2000) (codified at 16 C.F.R. pt. 313).

23. 15 U.S.C § 6802(a)(1) (2012) (requiring non-disclosure of "nonpublic personal information" to "nonaffiliated third parties").

24. *See* 15 U.S.C. §§ 6803(a), (c) (2012).

25. 15 U.S.C. §§ 1681–1681x (2012).

26. Pub. L. No. 100–618, 102 Stat. 3195. *See generally* Mollett v. Netflix, Inc., 795 F.3d 1062 (9th Cir. 2015). For more examples of narrow, sectoral legislation *see* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1440–44 (2001).

27. *See, e.g.*, Press Release, Sen. Ed Markey, Sens. Markey & Hatch Reintroduce Bipartisan Legislation to Protect Student Privacy (May 13, 2015), http://www.markey.senate.gov/news/press-releases/sens-markey-and-hatch-reintroduce-bipartisan-legislation-to-protect-student-privacy [https://perma.cc/AD5Y-7JP9].

28. Press Release, Sen. Ed Markey, Sens. Markey, Blumenthal Introduce Legislation to Protect Drivers from Auto Security, Privacy Risks with Standards & "Cyber Dashboard" Rating System (July 21, 2015), http://www.markey.senate.gov/news/press-releases/sens-markey-blumenthal-introduce-legislation-to-protect-drivers-from-auto-security-privacy-risks-with-standards-and-cyber-dashboard-rating-system [https://perma.cc/2ZMZ-BMWA].

29. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281/31), http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046 [https://perma.cc/S49Z-VL4V].

30. Commission Regulation 2016/679 of the European Parliament and of the Council of 27

notification[32] provisions. However, arguably one of its most significant achievements is to make enforcement and interpretation more consistent across the EU by designating a primary, "one-stop shop" regulator[33] and promoting additional coordination through the European Data Protection Board.[34]

Of course, the observation that U.S. data protection is flawed because of its sectoral nature is only part of the story. The sectors (including health care) are narrowly defined. After conventional health and, arguably[35] financial services, the drop off in protections is sharp. In large part, this is because the United States has favored relatively-low-protection models, most of which are downstream.

B. Upstream vs. Downstream Protection Models

The upstream-downstream typology described here may appear somewhat complex. However, its origins can be traced to a much simpler relationship—that between privacy and confidentiality. According to Tom Beauchamp and James Childress:

> [A]n infringement of a person's right to confidentiality occurs only if the person or institution to whom the information was disclosed in confidence fails to protect the information or deliberately discloses it to someone without first-party consent. By contrast, a person who, without authorization, enters a hospital record room or computer database violates rights of privacy but does not violate rights of confidentiality. Only the person or institution that obtains information in a confidential relationship can be charged with violating rights of confidentiality.[36]

This description captures a clear process chronology. First, "privacy"

April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 (General Data Protection Regulation), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC [https://perma.cc/R5NP-FR2Z].

31. *Id.* art. 17.

32. *Id.* arts. 33–34.

33. *Id.* arts. 56–65.

34. *Id.* arts. 68–76.

35. *Cf.* Kathleen A. Hardee, *The Gramm-Leach-Bliley Act: Five Years After Implementation, Does The Emperor Wear Clothes?*, 39 CREIGHTON L. REV. 915 (2006).

36. TOM L. BEAUCHAMP & JAMES F. CHILDRESS, PRINCIPLES OF BIOMEDICAL ETHICS 316–17 (7th ed. 2013); *see also* Humphers v. First Interstate Bank of Oregon, 696 P.2d 527 (Or. 1985) ("Although claims of a breach of privacy and of wrongful disclosure of confidential information may seem very similar in a case like the present, which involves the disclosure of an intimate personal secret, the two claims depend on different premises and cover different ground . . . [T]he most important distinction is that only one who holds information in confidence can be charged with a breach of confidence. If an act qualifies as a tortious invasion of privacy, it theoretically could be committed by anyone.")

protects against the unauthorized collection of health-care data. Subsequently, once the collection has been authorized, the recipient subsequently owes a duty of "confidentiality" not to disclose the data. That is, privacy (different flavors of which either prohibit or place limitations or conditions on the collection of data) protects data upstream of confidentiality.

Thus, the lifecycle of data can be mapped to a timeline-based typology. That typology may be expanded beyond "privacy" and "confidentiality" to include other data-protective models including core FIPPS, such as transparency, individual participation (including consent, access, correction, and redress), purpose specification, data minimization, use limitation, data quality and integrity, security, accountability, and auditing.[37] In broad terms, models that are applicable before or during collection are labeled "upstream," while those applied post-collection are labeled "downstream."

To privacy (upstream) and confidentiality (downstream) I now add some other basic data protection models (which may or may not be deployed by ethical, legal, or technological systems) such as anonymization, de-identification,[38] breach notification, inalienability, point-of-use regulation, or security.

Anonymizing data prior to any collection or using something like an inalienability or market inalienability[39] rule to reduce the use case/value of the data will tend to reduce the likelihood that the data are collected.

Upstream Models	
Model	**Detail**
Anonymization	Mandates removal of certain identifiers *before* data can be collected
Inalienability	Prohibits transfer of certain data, thus reducing their value and disincentivizing collection
Privacy	Prohibits or places limitations or conditions on the collection of data

37. *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy*, WHITE HOUSE 45 (April 2011), https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf [https://perma.cc/7JH3-MX7P].

38. While anonymization removes all associations between data and data subject, de-identification removes only select associations, leaving open the possibility, however slight, of re-identification. *See generally* Simson L. Garfinkel, *De-Identification of Personal Information*, U.S. DEP'T COM. NAT. INST. STANDARDS TECH., 2 (October 2015), http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf [https://perma.cc/Q898-QD5K].

39. *See generally* Margaret Jane Radin, *Market-Inalienability*, 100 HARV. L. REV. 1849 (1987).

In contrast, point-of-use regulation (such as the prohibition of discriminatory uses), security, and breach notification are downstream, post-collection protective models.

Downstream Models	
Model	**Detail**
Point-of-Use Regulation	Prohibits the use of legally collected data for certain (typically discriminatory) purposes
Security	Requires perimeter, encryption, or behavioral controls to impede unauthorized data access
Confidentiality	Prohibits data disclosure by data custodian or limits disclosure to certain persons or for certain purposes
Breach Notification	Obligates data custodian to disclose data compromise to data subject and/or regulator

This basic upstream-downstream relational structure may now be expanded to include other protective sub-models and also cross-walked to FIPPS.

Characteristic	Data Protection Model	Sub-Models/FIPPS
Upstream	Anonymization	
	Inalienability	
		Market Inalienability
	Privacy (Broad Control of Collection)	
		Control/Consent
		Purpose Specification
		Data Minimization/Proportionality
		Transparency
Downstream	Right of Erasure	
		De-linking

Point of Use Regulation	
	Non-discrimination
	Purpose limitation
Security	
	Accounting/Audit
	Quality & Integrity
Confidentiality (Broad Control of Disclosure)	
	Use Limitation
	Quality & Integrity
	Anonymization
	De-identification
	Pseudonymization
	Suppression
	Perturbation
	Prohibitions on Reidentification
	Transparency
	Access/Accuracy/Correction
	Accounting/Audit
Breach Notification	

This more complex representation also reflects that some protections (for example, transparency or, where they overlap, anonymization and de-identification) can occur at multiple times in the lifecycle of the data. Note also that some sub-models are complimentary. For example, the upstream privacy (collection) sub-model that prohibits collection of data other than for a disclosed purpose would likely be complemented by a downstream prohibition on disclosure other than for the stated purpose.

I suggest several interrelated takeaways from this typology. First, and most obviously, policymakers (or, for that matter, data custodians) can and *should*

choose from a broad array of data protection models. Having a comprehensive toolbox should help regulators finely calibrate their approach to particular data risks and help them be prepared to deal with evolving or currently unknown data risks.

Second, a broad understanding of the various data protection models *and* their relative approaches to protecting data should make it less likely that policymakers and data custodians will resort to generalized statements about protecting data. For example, those who use "privacy" rhetoric should have their feet held to the fire about the specifics of their calls for more or less data protection.

Third, the complexity of this typology is worthwhile if it helps push back against the tendency to reduce policy discussions to binaries or other over-simplifications. Even a creaking common law found room for both privacy and confidentiality models, while today policymakers and regulators can choose from an array of upstream and downstream data protection models. For example, it has been common for mainstream data protection proposals to exclude data or data custodians subject to HIPAA.[40] However, once it is appreciated that HIPAA is a downstream confidentiality model, it makes sense to *include* health care in discussions about the adoption of future *upstream* protective models.

Finally, this typology locates health-care data protection within the mainstream of data protection. Mainstream data protection should embrace health-care data protection as one of its own and learn from its experiences. The resolutely downstream, highly detailed, prescriptive HIPAA privacy rule is unique and the law and policy literature surrounding it is robust. This is a two-way street. As argued below, health-care data protection needs to move beyond its HIPAA-centricity and see what additional models could be used to protect health-care data generated or used both inside and outside of traditional health-care environments. Non-health-care domains, conversely, should learn from health care's twenty years of experience with HIPAA.

II. REGULATORY TURBULENCE, DISRUPTION & ARBITRAGE

Regulatory turbulence, disruption, and arbitrage presuppose the juxtaposition of at least two regulatory domains. In the simplest case, one domain would be regulated, the other unregulated. Turbulence and disruption exist on a continuum. Regulatory turbulence may be only transient or, in the scheme of things, relatively benign. Regulatory disruption has more permanent and serious

40. *See, e.g.*, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FED. TRADE COMMISSION, i-v (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/VJ9Q-KQU4] [hereinafter *Protecting Consumer Privacy*]; *Framework for Protecting Privacy*, *supra* note 18, at 38.

implications. Regulatory arbitrage occurs when a business purposefully exploits disruption, making business choices on the basis of the difference between the two regulatory domains.

A slightly different way to think about these phenomena is to posit horizontal and vertical products. Turbulence and disruption occur when horizontal business products (for example, cloud services or smartphone platforms) are dropped into vertical markets without regard to potentially unique regulatory issues. On the other hand, arbitrage tends to occur when a business is aware of a vertical market's unique regulation and builds a surrogate or proxy business in a less regulated vertical market.

A. Turbulence and Disruption

Regulatory turbulence, disruption and potentially arbitrage will most likely occur following some type of business disruption. True to Clayton Christensen's classic disruption theory,[41] such a business disruption frequently occurs because a disruptive technological innovation has empowered an entrant attacker to challenge mainstream industry incumbents.[42] Disruptive technologies may initially underperform (or undershoot) incumbents' sustaining technologies. However, disruptive technologies "are typically cheaper, simpler, smaller, and, frequently, more convenient to use."[43] Business disruption can also include "[n]ew-market disruptive innovations," which "occur when characteristics of existing products limit the number of potential consumers or force consumption to take place in inconvenient, centralized settings."[44]

Regulatory turbulence and disruption tend to develop in parallel with or soon after business disruption. Take ride-hailing services typified by Uber[45] or Lyft.[46] They generally obey the business disruption model. Incumbent taxi services, although featuring (apparently) professionally-trained drivers, access at major locations, and liveried cabs, rely on sustaining technologies such as telephone bookings or in-person ride-hailing, and cash or often poorly implemented credit card payments. Disruptive ride-hailing services leverage spare capacity in private owners' vehicles, ubiquitous mobile communication, expanded locations, and payment services to deliver nimbler, more convenient services. The core "assets"

41. *See, e.g.*, CLAYTON M. CHRISTENSEN, THE INNOVATOR'S DILEMMA: WHEN NEW TECHNOLOGIES CAUSE GREAT FIRMS TO FAIL (1997).

42. *See generally* Nicolas P. Terry, *Information Technology's Failure to Disrupt Health Care*, 13 NEV. L.J. 722 (2013).

43. CHRISTENSEN, *supra* note 41, at xv.

44. CLAYTON M. CHRISTENSEN ET AL., SEEING WHAT'S NEXT: USING THE THEORIES OF INNOVATION TO PREDICT INDUSTRY CHANGE xvii (2004).

45. UBER TECHNOLOGIES, INC., https://www.uber.com [https://perma.cc/7R88-X93Q].

46. LYFT, INC., https://www.lyft.com [https://perma.cc/7AY4-T2VL].

of ride-hailing or housing (such as Airbnb[47]) businesses are traditionally-underused resources that modern technologies can easily make available to a "sharing economy." In addition, their business models clearly embrace regulatory disruption.

Ride-hailing services initially caused regulatory turbulence, based on uncertainty as to whether they were subject to existing regulatory models. Indeed, this appeared to be a deliberate part of their disruptive strategy. Uber, in particular, challenged local regulations or argued they were ambiguous. Their CEO noting in 2013: "It's a regulatory disruption . . . We don't talk about that a lot in tech. But you can disrupt from all sorts of directions."[48] These businesses, whether sharing unused automobile or housing resources, at the root are adopting business models that seek to reduce costs relative to incumbent competitors by avoiding or marginalizing self-regulatory organizations (such as guilds[49]), governmental rationing (such as medallions[50]), or regulatory models (such as licensure[51] or employment laws[52]).

Initial regulatory turbulence buys time during which the innovator can press for accommodating regulatory compromises (that themselves further continued

47. AIRBNB, INC., https://www.airbnb.com [https://perma.cc/5XQ8-LEV9].

48. *Uber CEO Talks Regulatory Disruption, Maintaining Startup Culture*, MIT SLOAN MGMT. (Nov. 6, 2013), http://mitsloan.mit.edu/newsroom/articles/uber-ceo-talks-regulatory-disruption-maintaining-startup-culture [https://perma.cc/NG3C-XWC7].

49. *See generally* Justin Fox, *The Problem with Guilds, from Silversmiths to Taxi Drivers*, HARV. BUS. REV. (Dec. 4, 2014), https://hbr.org/2014/12/the-problem-with-guilds-from-silversmiths-to-taxi-drivers [https://perma.cc/G5YR-45H5]; *see also*, Erik Engquist, *Judge Rules on Taxi Industry Lawsuit: Compete with Uber or Die*, CRAIN'S N.Y. BUS. (Sept. 9, 2015), http://www.crainsnewyork.com/article/20150909/BLOGS04/150909863/judge-rules-on-taxi-industry-lawsuit-compete-with-uber-or-die [https://perma.cc/E7D4-T2NE].

50. Aamer Madhani, *Once a Sure Bet, Taxi Medallions Becoming Unsellable*, USA TODAY (May 18, 2015), http://www.usatoday.com/story/news/2015/05/17/taxi-medallion-values-decline-uber-rideshare/27314735 [https://perma.cc/VD9D-NJ65].

51. *See, e.g.*, Colleen Wright, *Uber Says Proposed Freeze on Licenses in New York City Would Limit Competition*, N.Y. TIMES (June 30, 2015), http://www.nytimes.com/2015/07/01/nyregion/uber-says-proposed-freeze-on-licenses-would-limit-competition.html [https://perma.cc/R2MN-JU39]; *see also* Sebastian Anthony, *London Mayor Says Uber Is Systematically Breaking the Law*, ARS TECHNICA (Oct. 5, 2015), http://arstechnica.com/cars/2015/10/boris-johnson-says-uber-is-systematically-breaking-the-law-in-london [https://perma.cc/7SGM-R4XN]; Leon Daniels, *Transport for London: Uber and London's Private Hire Trade Need New Regulations*, CITY A.M., LTD. (Oct. 20, 2015), http://www.cityam.com/226929/transport-for-london-uber-and-londons-private-hire-trade-need-new-regulations [https://perma.cc/7AR2-8DCW]. Leah Thorsen, *Defying Regulators, Uber Launches Service, Files Lawsuit*, STLTODAY.COM (Sept. 19, 2015), http://www.stltoday.com/business/local/uber-sues-st-louis-taxicab-commission-launches-service-without-approval/article_42b7f122-b8a6-536f-ba68-6acef3503075.html [https://perma.cc/DC7W-UAQY].

52. *See, e.g.*, Sean Buckley, *California Unemployment Office Says Uber Driver was an Employee*, ENGADGET (Sept. 11, 2015), http://www.engadget.com/2015/09/11/california-unemployment-office-says-uber-driver-was-an-employee [https://perma.cc/UX3X-453C].

disruption) or create or exploit regulatory gaps (enabling regulatory arbitrage).[53] All the while, the disruptive services and their technologies mature, cease undershooting the incumbents, and gain popularity and market share that regulators will fear to reverse.[54] Former White House aide Ron Klain describes the phenomenon as follows:

> [W]hat these Internet 3.0 companies are disrupting is not really technology, but regulatory regimes. What makes AirBnb exceptional is not any technological breakthrough, but how it is challenging local hospitality regulation, condo board rules, and all the other limitations on who can charge what and when for short-term housing usage. Crowdfunding sites likewise use technology that has been around for years: what they are disrupting is the vast array of federal and state regulations that govern who can invest in what, and under what terms. The same is true of so many other emerging Internet companies: their impact is far more in disrupting governmental and quasi-governmental rules than it is in technological breakthroughs.[55]

While policy and political allegiances slowly determine a regulatory re-calibration, incumbents and attackers operate in an uneven, even incoherent regulatory system that applies different rules to what should be competing services.

In the health-care space, some service providers claim or are hailed as having Uber-like characteristics. For example, *American Well* promises 24x7 doctor consultations,[56] while *Heal*[57] and *pager*[58] promise timely house calls by a physician. However, these are far less disruptive than they appear at first sight. They generally are respectful of regulatory systems and while leveraging mobile technologies do not attack incumbents' features, such as third party

53. *Cf.* Amar Toor, *Uber Drivers Stage Protest over French Response to Taxi Strike*, VERGE (Feb. 3, 2016), http://www.theverge.com/2016/2/3/10903662/uber-protest-paris-taxi-strike-vtc [https://perma.cc/N448-SYDD].

54. Of course, there are exceptions. *See* Mark Scott, *Uber's No-Holds-Barred Expansion Strategy Fizzles in Germany*, N.Y. TIMES (Jan. 3, 2016), http://www.nytimes.com/2016/01/04/technology/ubers-no-holds-barred-expansion-strategy-fizzles-in-germany.html [https://perma.cc/Q4GT-3S58].

55. Ron Klain, *Airbnb's Biggest Disruption: America's Laws*, FORTUNE (Sept. 10, 2014), http://fortune.com/2014/09/10/airbnbs-biggest-disruption-americas-laws [https://perma.cc/MJY3-U2PX].

56. AMERICAN WELL, https://www.americanwell.com/how-it-works [https://perma.cc/5B5Q-JZXT].

57. *What is Heal?*, HEAL, https://help.getheal.com/hc/en-us/articles/204181405-What-is-Heal [https://perma.cc/248B-3WKQ]; *see generally* Kavita Daswani, *Feeling Sick? How About a House Call from a Doctor? A New App, Heal, Makes it Happen*, L.A. TIMES (Nov. 7, 2015), http://www.latimes.com/health/la-he-heal-at-home-20151107-story.html [https://perma.cc/MC8X-QF99].

58. PAGER, https://pager.com [https://perma.cc/L4WK-WQJG].

reimbursement. So far, they have opted for more of a concierge model that has limited scalability.

Indeed, business disruption has generally failed in the health-care space. The most conspicuous failure has been Google's failed challenge to the data hegemony of incumbent health-care entities by offering low-cost personal health records (PHRs).[59] The low level of business disruption probably explains the relatively low level of regulatory turbulence or disruption in the domain, at least until recently.

There are several reasons why technology companies have found health care difficult to disrupt. The dominant reason is health care's primary financing model. "Third-party reimbursement systems sap motivation for innovation—particularly disruptive innovation—out of the system."[60] However, there are additional, deep-seated causes. Thus, the "meaningful use" debacle suggests that while market failure was one explanation for the slow adoption of Electronic Health Records (EHRs), underperforming products may have been as salient.[61] Further, information technologies may not be a good fit for current, unreformed health care. Information technology maps best to processes, not health care's flawed episodic nature. Additionally, information technologies thrive on liquid data, which health care still struggles to promote.[62] It is also possible that technology companies, perhaps fooled by the presence of vertical integration and positive outliers (such as the VA or Kaiser Permanente), underestimated the challenge of changing culturally constipated, heterogeneous providers.

Notwithstanding the absence of direct business disruption, two phenomena, big data collection and mobile health, are proving to be indirectly disruptive—with the potential to move into a more direct mode. Indeed, the argument can be made that mobile health is an example of Uber-like regulatory disruption or "uberfication," a disruptive, tech-heavy approach that promotes "uber-convenience" through always-on mobile services that instantly match patient demand with health-care supply. Both mobile health and big data analytics have developed primarily outside of (and sometimes in parallel to) traditional health-care spaces. As their overlaps increase, however, they are also providing technologically-mediated alternatives to traditional health-care interactions, services, and data. In this regard, they offer the potential for business disruption. As discussed below, they are already disrupting regulatory models and exhibiting some arbitrage.[63]

---

59. *See infra* text accompanying note 117.

60. CHRISTENSEN, *supra* note 44, at 197.

61. Nicolas P. Terry, *Pit Crews With Computers: Can Health Information Technology Fix Fragmented Care?*, 14 HOUS. J. HEALTH L. & POL'Y 129, 168–75 (2014).

62. *Id.*

63. *See infra* text accompanying note 196, 212.

B. Arbitrage

In Victor Fleischer's words, regulatory arbitrage "exploits the gap between the economic substance of a transaction and its legal or regulatory treatment . . ."[64] However, Fleischer was primarily interested in "regulatory gamesmanship" and modeling the tradeoff between regulatory and transaction costs. The examination of regulatory arbitrage in this article more closely resembles leveraging differences in regulatory substance between different jurisdictions. A well-known example is the "double-Irish," when a taxpayer shifts income out of a high-tax jurisdiction into a tax haven.[65] Examples in the health-care domain would include Israeli gays, prohibited by domestic law from using surrogacy, employing third world surrogates instead,[66] a UK resident avoiding a health-care shortage (wait-list) by having the procedure performed elsewhere in the European Union and subsequently requiring the UK to reimburse them,[67] and providers attracting patients to jurisdictions where CRISPR-Cas gene editing is available.[68]

Of course, the issue discussed herein is not transnational, but rather domestic arbitrage that exploits variances between U.S. regulatory silos. An evolving example of domestic regulatory disruption or arbitrage in our health-care domain is the growing "off-label use" of FDA approved drugs. Two "disruptions" enabled the regulatory arbitrage. First, business disruption created massive (and highly profitable) markets for unapproved uses. Second, the legal disruption (or "First Amendment opportunism"[69]) caused by the rapid development of (commercial) speech jurisprudence.[70]

---

64. Victor Fleischer, *Regulatory Arbitrage*, 89 TEX. L. REV. 227, 229 (2010).

65. *See, e.g.*, *Death of the Double Irish*, ECONOMIST (Oct. 18, 2014), http://www.economist.com/news/finance-and-economics/21625876-irish-government-plans-alter-one-its-more-controversial-tax [https://perma.cc/NTS3-JEPT]; *see generally* Annelise Riles, *Managing Regulatory Arbitrage: A Conflict of Laws Approach*, 47 CORNELL INT'L L.J. 63 (2014).

66. Ruth English, *Among Nepal's Earthquake Survivors: Israeli Gays and Their Surrogate Babies*, WASH. POST (Apr. 30, 2015), https://www.washingtonpost.com/world/how-an-earthquake-highlighted-the-plight-of-israeli-gays-and-their-surrogate-babies/2015/04/29/419d60e8-ecf0-11e4-8050-839e9234b303_story.html [https://perma.cc/39M7-P964].

67. *See* C-372/04, Watts v. Bedford Primary Care Trust, 2006 E.C.J. I-04325; *see generally* Nicolas P. Terry, *Under-Regulated Healthcare Phenomena in a Flat World: Medical Tourism and Outsourcing*, 29 W. NEW ENG. L. REV. 421–72 (2007).

68. *See, e.g.*, R. Alta Charo, *On the Road (to a Cure?)—Stem-Cell Tourism and Lessons for Gene Editing*, 374 NEW ENG. J. MED. 901 (2016).

69. FREDERICK SCHAUER ET AL., ETERNALLY VIGILANT: FREE SPEECH IN THE MODERN ERA 175–76 (Lee C. Bollinger & Geoffrey R. Stone eds., 2001).

70. *See, e.g.*, Sorrell v. IMS Health Inc., 131 S.Ct. 2653 (2011). *See generally* Jennifer M. Keighley, *Can You Handle the Truth? Compelled Commercial Speech and the First Amendment*, 15 U. PA. J. CONST. L. 539 (2012); Robert Post, *Transparent and Efficient Markets: Compelled Commercial Speech and Coerced Commercial Association in United Foods, Zauderer, and Abood*, 40 VAL. U. L. REV. 555 (2006). *See also* Aaron S. Kesselheim, *Off-Label Drug Use and Promotion: Balancing Public Health Goals and Commercial Speech*, 37 AM. J.L. & MED. 225 (2011).

In *U.S. v. Caronia*, the Second Circuit overturned the conviction of a drug representative for promoting an off-label use of a central nervous system depressant. Applying strict scrutiny, the court held the government could not prosecute manufacturers or representatives for speech promoting the lawful, off-label use of an approved drug.[71] Dissenting, Judge Livingston recognized the regulatory disruption caused by her colleagues. "[T]he majority calls into question the very foundations of our century-old system of drug regulation."[72] The court described the regulatory gap exploited by the drug company as follows: "[t]o obtain FDA approval, drug manufacturers are required to demonstrate, through clinical trials, the safety and efficacy of a new drug for each intended use or indication" but that "[o]nce FDA-approved, prescription drugs can be prescribed by doctors for both FDA-approved and -unapproved uses; the FDA generally does not regulate how physicians use approved drugs."[73] By marketing its regulated drug to unregulated (in this context) physicians, the drug company created regulatory disruption. Subsequently, in *Amarin Pharma, Inc. v. FDA*, a district court rejected FDA's narrow reading of *Caronia* and enjoined the agency from threatening a misbranding action in another off-label use case because it chilled protected speech.[74] One of the FDA's goals in pursuing such actions is to "encourage use of the FDA's drug review and approval process" and "deter manufacturers from evading the FDA's review process for additional uses of approved drugs."[75] By leveraging the differential regulatory models applied to drug manufacturers and doctors, the industry is avoiding that very process.

C. Implications of Regulatory Disruption and Arbitrage

As discussed above, using ride-hailing and accommodation-sharing services as examples, regulatory turbulence tends to create uncertainty, which increases information costs among market participants, policymakers, and regulators. This may be followed by far more serious regulatory disruption where incumbents and attackers face uneven policy environments. These *de facto* differential regulatory environments may be a product of non-enforcement by regulators. For example, regulators may exercise discretion for fear of, say, frustrating innovation or the political cost of "interfering" with a popular new service. Equally, in an attempt

71. 703 F.3d 149, 169 (2nd Cir. 2012).

72. *Id.*

73. *Id.* at 153 (citations omitted).

74. 119 F. Supp. 3d 196 (S.D.N.Y. 2015). Subsequently Amarin and FDA settled the case. Order of Settlement, Amarin Pharma, Inc. v. FDA, 119 F. Supp. 3d 196 (S.D.N.Y. 2015) (No. 1:15-CV-03588). *See also* Kathleen M Sanzo, Lisa D. Dykstra & Jacqueline R. Berman, *FDA and Amarin Reach Settlement on First Amendment and Off-Label Statements*, NAT'L L. REV. (Mar. 10, 2016), http://www.natlawreview.com/article/fda-and-amarin-reach-settlement-first-amendment-and-label-statements [https://perma.cc/7GYE-LDTR].

75. *Amarin*, 119 F. Supp. 3d at 205.

to deal temporarily with disruption during a time of policy recalibration, agencies might issue sub-regulatory "guidances." Seeking to be supportive of both incumbents and innovators can be unclear, so the regulatory guidances create ambiguity and therefore increase disruption. In the data space, regulatory disruption does not stop with similar data being subject to differential regulation. Additionally, data subjects may experience regulatory "churn" during their lifecycle, as data repeatedly enter or exit regulated and lightly regulated spaces (or even exist in both spaces simultaneously), further adding to the information costs in identifying a current regulatory state.

III. EXCEPTIONALISM AND THE HEALTH-CARE DATA PROTECTION MODEL

HIPAA has been one of the most consistently criticized regulatory constructs in the health-care sector.[76] Yet, its levels of data protection and enforcement likely would provoke envy from data subjects in other domains. HIPAA provides relatively robust protections against unauthorized uses of health information by a relatively narrow set of traditional health-care provider data custodians. Its inherent limitations are because of its narrow domain inclusions (some traditional health-care providers and insurers, *not* all custodians of health-care data) and because it uses downstream data protection modes (that is, it does almost nothing to regulate the *collection* of health data). An accurately labeled HIPAA privacy rule would be something like "the doctor/hospital/insurer" confidentiality rule. The other HIPAA rules—security and breach notification—have the same limitations; U.S. health-care data protection is not only sectoral, but also almost completely downstream.

A. Sectoral Model

As noted by the White House report on big data, "[i]n the United States during the 1970s and 80s, narrowly-tailored sectoral privacy laws began to supplement the tort-based body of common law. These sector-specific laws create privacy safeguards that apply only to specific types of entities and data."[77] When HIPAA was originally drafted, there was every reason to believe that the domain-limited model was intended, in large part, to separate health-care data

76. *See, e.g.*, Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681 (2007); Nicolas P. Terry, *What's Wrong with Health Privacy?*, 5 J. HEALTH & BIOMEDICAL L. 1 (2009). More recently, *see* Charles Ornstein & Annie Waldman, *Few Consequences for Health Privacy Law's Repeat Offenders*, PROPUBLICA (Dec. 29, 2015), https://www.propublica.org/article/few-consequences-for-health-privacy-law-repeat-offenders [https://perma.cc/LD6S-FJNA]; Mark Rothstein, *The End of the HIPAA Privacy Rule?*, 44 J.L. MED. & ETHICS 352 (2016).

77. *Big Data: Seizing Opportunities, Preserving Values*, WHITE HOUSE 18 (May 2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [https://perma.cc/QTU9-6FB3] [hereinafter *Big Data: Seizing Opportunities*].

from financial services data.[78]

There could have been no misapprehension that all health-care data custodians would be covered by the rule given the limitations of the enabling legislation.[79] The likely proof is that the coverage of outsiders such as law firms and marketing companies had to be "patched" with mandatory contracts between insider-covered entities and their outsider "business associate."[80] It was not until 2009 when additional statutory authority provided by the Health Information Technology for Economic and Clinical Health (HITECH) Act[81] allowed for their direct regulation.[82] Similarly, it was apparent early on that neither life insurers, nor most employers[83] (except to the extent that they were also health plan administrators[84]) were covered. Those exceptions aside, HIPAA appeared to blanket health care, at least as we knew it in 1999. This was achieved using sector-specific language: "(1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction. . ."[85]

Ignoring the technical verbiage, HIPAA regulated health insurers and traditional health-care providers such as doctors, hospitals and pharmacists.[86] A couple of other limitations to the definition of protected data minimally reduced the ranks of regulated providers. For example, the requirement of transmittal of "any health information in electronic form"[87] may have excluded some technologically limited, often rural providers.

Other exclusions are more implicit. For example, only "individually identifiable health information"[88] is protected, and "[h]ealth information that does not identify an individual . . . is not individually identifiable health information."[89] As a result, de-identified data are not subject to HIPAA regulation. De-identification may be achieved by the use of the expert (aka

78. *See infra* text accompanying note 133 *et seq.*

79. The legislation primarily was concerned with imposing e-commerce models on those engaged in traditional health-care transactions. Hence, the regulatory authority was limited to providers, insurers and clearinghouses. *See* HIPAA Act of 1996, Pub. L. No. 104-191, § 262, 110 Stat. 1936, 2021–31 (codified in scattered sections of 42 U.S.C.).

80. 45 C.F.R. §§ 160.103, 164.502(e), .504(e), .532(d)(e) (2016).

81. Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Pub. L. No. 111-5, § 13401, 123 Stat. 115, 260.

82. *See* 45 C.F.R. § 160.102(b) (2016).

83. 45 C.F.R. § 160.102 (2015) (protected health information).

84. 45 C.F.R. § 164.504(f) (2016).

85. 45 C.F.R. § 160.102 (2016).

86. For a broad critique of the limitations of HIPAA's reach, *see* Terry & Francis, *supra* note 76, at 713–17.

87. 45 C.F.R. § 160.103 (2016) (covered entity).

88. 45 C.F.R. § 164.103 (2016).

89. 45 C.F.R. § 164.514 (2016).

statistical) method[90] or the removal of certain identifying elements so as to trigger a safe harbor.[91] Furthermore, an Institutional Review Board (IRB) can, in limited circumstances, act as a surrogate for individuals and waive consent/authorization for the use of identifiable data for research purposes.[92] Taken together, these provisions suggest that most, but not all,[93] researchers fall outside of HIPAA regulation, their use of data instead being subject to the Common Rule.[94]

As a result, HIPAA's own "original sin" is easy to identify. The data protection model is structured around a group of identified health-care data custodians rather than around health-care data. Although HITECH expanded direct applicability and enforcement to business associates in 2009, it granted no additional expansion of the Privacy or Security Rules to deal with health-care data existing outside of the HIPAA-zone. There was one exception: the nature of which illustrated rather than solved the HIPAA deficit. HITECH provided for a breach notification rule applicable to the providers of PHRs by some non-HIPAA-regulated entities. However, it did not extend the HIPAA rule[95] to them; instead, it provided for distinct FTC rule-making for this limited group of non-HIPAA entities.[96] This approach therefore highlights two of the problems associated with sectoral models: fragmentation of data protection by custodian type and sector/sub-sector-specific regulators.

B. Downstream Protection Favored

Contemporary health-care data protection is resolutely and almost exclusively downstream. The HIPAA Privacy Rule employs a downstream data protection model ("confidentiality") that seeks to contain the collected data within the health-care system by prohibiting its migration to non-health-care parties.[97] Its complementary Security Rule imposes physical and technological constraints on patient data storage designed to impede those outside of the health-care system from acquiring such data without consent.

The only upstream protection in HIPAA, patient consent at initiation of the provider-patient relationship was, as discussed below,[98] removed even before the

90. 45 C.F.R. § 164.514(b)(1) (2016).

91. 45 C.F.R. § 164.514(b)(2) (2016).

92. 45 C.F.R. § 164.512 (2016).

93. *Cf.* 45 C.F.R. § 164.514(e) (2016) (limited data set recipients).

94. *See generally Federal Policy for the Protection of Human Subjects ('Common Rule')*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/ohrp/humansubjects/commonrule [https://perma.cc/273L-SGT2].

95. HITECH Act § 13402, 42 U.S.C. § 17932 (2012) (Omnibus Rule).

96. HITECH Act § 13407, 42 U.S.C. § 17939 (2012) (Health Breach Notification Rule).

97. *See, e.g.*, 45 C.F.R. § 164.502 (2016).

98. *See infra* text accompanying note 138.

Privacy Rule came into effect. In modern law, HIPAA aside,[99] only one health-care data-protection law, the Genetic Information Nondiscrimination Act of 2008 (GINA),[100] has exhibited any upstream modeling.[101]

Historically, some upstream, collection-centric data protection models, such as the intentional tort of intrusion into seclusion, have seen limited application in the health-care domain. However, these have experienced only limited build-out. Thus, the seclusion tort seems most comfortable when applied to obviously intentional outlying factual situations such as unconsented-to photography by physicians.[102] Routinely, now, courts seem to prefer the downstream breach of confidence tort as the dominant common law model of health-care data protection.[103]

Even aside from aligning with the prevalent model of U.S. data protection, it is not hard to explain why health-care data protection opted for a downstream path. Historically, the culture of medicine has seemed to favor collecting *everything*. Such a model was largely uncomplicated given the available technologies and diagnostic practice. It was also largely uncontroversial in the context of a traditional, two-party physician-patient relationship; the patient exercised his or her autonomy rights and disclosed all data to the physician in return for more effective treatment and a promise of confidentiality. It is hard to imagine that upstream FIPPS such as context or data minimization would have been explored in this simple health-care data exchange scenario. Rather, any conflicts that arose would tend to be dealt with in the framework of restrictions on data disclosure and the reach of exceptions from it.

It should have been relatively obvious that this model would not scale well to industrial health care. It is not particularly surprising that the eventual federal model would persist with downstream protections—it was after all based on state common law and statutes that also were primarily downstream. Even the latest addition to the health-care data protection regime, the quintessentially downstream breach notification rule introduced in 2009, was likely inspired by

99. This is something of an exaggeration as HIPAA and GINA are tied together in some places, such as by the provisions of the HITECH Act.

100. Pub. L. No. 110–233, 122 Stat. 881 (2008).

101. *See infra* text accompanying note 148 *et seq.* One reviewer made the interesting observation that medical data used in research may be subject to some upstream regulation under the Common Rule, 45 C.F.R. pt. 46. This seems correct in at least two situations. First, some research involving vulnerable populations (such as children or prisoners) is prohibited or regulated so strictly that it may be impractical. Second, unlike clinical data, the Common Rule does require consent prior to the collection or use of data and therefore does operate upstream.

102. *See, e.g.*, McCormick v. England, 494 S.E.2d 431, 435 (S.C. Ct. App. 1997); Burger v. Blair Med. Assocs., 964 A.2d 374, 379 (Pa. 2009); *see also* Susan Candiotti & Alan Duke, *Source: Joan Rivers' Doctor Took Selfie, Began Biopsy Before Her Cardiac Arrest*, CNN (Nov. 11, 2014), http://www.cnn.com/2014/09/16/showbiz/joan-rivers-clinic [https://perma.cc/G5CX-NCCD].

103. *See, e.g.*, Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 523 (Ohio 1999); Humphers v. First Interstate Bank of Oregon, 696 P.2d 527 (Or. 1985).

state models given the absence of any federal example. The shift from individual to institutional care also highlights a cultural peculiarity with regard to data "ownership" or its control. While the pre-industrial model was an informal sharing of responsibilities between physician and patient, joint ownership did not survive the transition. Today, it is providers who own and control patient data. Indeed, this is the premise behind HIPAA privacy and security. This is not only different from the more individual human rights-based protections recognized in non-US data protection frameworks, but also a major hurdle as reformers seek to engage patients in their health care, including their data.[104]

Additionally, health-care data protection has appeared increasingly blind to the impact of information technology. Looking through the health-care industry lens this should not be too surprising. Almost every contemporary technological challenge thrown at the health-care industry—Y2K,[105] the HIPAA transactional mandate,[106] HIT adoption,[107] Meaningful Use,[108] and ICD-10[109]—have been met with objection and prevarication.[110]

While it seems a truism that the common law has marched "with medicine but in the rear and limping a little,"[111] the lag of regulation in the face of information technology has been even more marked. If the HIPAA architects thought they had a fairly good grasp on the health-care domain in the 1990s, thereafter the vector between regulation and technology has increased considerably. In hindsight, perhaps the greatest flaw in HIPAA is that it takes a pre-IT (maybe even pre-industrialized medicine) approach to data use; it is either permitted or prohibited. That binary may have been appropriate for the limited records of the Marcus Welby, M.D.-era.[112] At the time the HIPAA rules were first promulgated, EHRs were barely visible and HHS was chasing e-commerce

104. See *infra*, discussion of "Blue Button," text accompanying note 175 *et seq.*

105. *See generally* Lily Rothman, *Remember Y2K? Here's How We Prepped for the Non-Disaster*, TIME (Dec. 31, 2014), http://time.com/3645828/y2k-look-back [https://perma.cc/R6ZZ-Z7SK].

106. *Transactions Overview*, CTRS. FOR MEDICARE & MEDICAID SERVS., https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Transactions/TransactionsOverview.html [https://perma.cc/EAG5-QCS9].

107. *See generally* Nicolas P. Terry, *Information Technology's Failure to Disrupt Healthcare*, 13 NEV. L.J. 722 (2013).

108. *See generally* Nicolas P. Terry, *Meaningful Adoption: What We Know or Think We Know About the Financing, Effectiveness, Quality, and Safety of Electronic Medical Records*, 34 J. LEGAL MED. 7 (2013).

109. *Data and Systems*, MEDICAID.GOV, https://www.medicaid.gov/medicaid-chip-program-information/by-topics/data-and-systems/icd-coding/icd.html [https://perma.cc/Y6ZK-E34C].

110. *See generally* Robert Wachter, *Meaningful Use: Born 2009 – Died 2014?*, HEALTHCARE IT NEWS (Nov. 13, 2014), http://www.healthcareitnews.com/blog/meaningful-use-born-2009-died-2014 [https://perma.cc/V8G9-CQS8].

111. *Mount Isa Mines v Pusey* (1970) 125 CLR 383, 395 (Austl.) (Windeyer J).

112. *See Marcus Welby, M.D.*, WIKIPEDIA, https://en.wikipedia.org/wiki/Marcus_Welby,_M.D. [https://perma.cc/6D3Q-DW2Z] (last modified Sept. 20, 2016).

models that were already well-established a decade before in other domains. The cycle then seemed to repeat. By 2009, the country was in the middle of a federal initiative to bring EHRs to all hospitals and the same legislation authorized an expensive subsidy program to catch-up.[113] Yet, most of the data protection provisions in HITECH were designed to correct or tweak ten-year-old flaws in HIPAA.[114]

The most "outside-the–box" provision in the HITECH Act was the discrete breach notification rule for non-HIPAA PHRs. This was the first acknowledgment that HIPAA-like data were being created or processed by data custodians who were not subject to HIPAA. For a brief period in the late 2000s, PHRs seemed poised to gain some traction as an alternative to the slowing Bush administration ten-year EHR initiative.[115] Of the PHRs that were launched in this period, *Google Health* was by far the most potentially disruptive. Indeed, it was a clear example of incipient regulatory arbitrage because Google intended to avoid HIPAA by dealing directly with patients (data subjects) rather than covered entities (regulated data custodians).[116] Shortly after Google *Health* launched, HITECH introduced the Meaningful Use program based around proprietary EHR formats. Google, its technical model built around open web standards, shuttered *Google Health*.[117] By the time most of the HITECH provisions found a regulatory form in the 2013 *Omnibus Rule*, the ball had moved again, with concerns being raised about big data and mobile health data. More recently, questions about health-care data protection also have been raised about the Internet of Things, described by the FTC, as "an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people."[118]

The sector-based approach to data protection has led to today's chronically uneven policy environment, causing, as discussed below, regulatory disruption and enabling arbitrage in the health-care domain. It is policymakers' over-

113. HITECH Act of 2009, Pub. L. No. 111-5, Title XIII, 123 Stat. 115, 226-79 (codified as amended in scattered sections of 42 U.S.C. (2012)).

114. The exception was section 13405(d) prohibiting certain sales of EHR data. *See also* 45 C.F.R. § 164.502(a)(5)(ii) (2016).

115. *Transforming Health Care: The President's Health Information Technology Plan*, WHITE HOUSE: PRESIDENT GEORGE W. BUSH (Jan. 20, 2004), http://georgewbush-whitehouse.archives.gov/infocus/technology/economic_policy200404/chap3.html [https://perma.cc/FHV6-DJYW].

116. Terry, *supra* note 107, at 745–46.

117. Aaron Brown & Bill Weihl, *An Update on Google Health and Google PowerMeter*, GOOGLE BLOG (June 24, 2011), http://googleblog.blogspot.com/2011/06/update-on-google-health-and-google.html [https://perma.cc/G3Z3-CVQK]. *See generally* Nicolas P. Terry, *Personal Health Records: Directing More Costs and Risks to Consumers?*, 1 DREXEL L. REV. 216 (2009).

118. *Internet of Things, Privacy & Security in a Connected World*, FED. TRADE COMMISSION 1 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/R94L-AP6C].

commitment to downstream rules that makes reform problematic, however. Arguably, tweaked downstream rules cannot deal with the challenges to health-care data protection; upstream models must also be deployed.

C. Understanding Exceptional Health-Care Data Protection

To an extent, health-care data privacy exceptionalism has enjoyed more legal recognition than health-care exceptionalism, although that may now be changing. The exceptional treatment of health care was dealt a blow in *National Federation of Independent Businesses v. Sebelius* when a Supreme Court majority rejected any special treatment under the Commerce or Necessary & Proper Clauses.[119] Yet, three years later in *King v. Burwell*, an exceptionalism argument found favor with the majority. There Chief Justice Roberts justified the adoption of a *Chevron* zero approach to interpretation of the Affordable Care Act[120] on the fact that the Act's insurance provisions raised issues of "deep 'economic and political significance.'"[121] The opinion later held: "Congress passed the Affordable Care Act to improve health insurance markets, not to destroy them. If at all possible, we must interpret the Act in a way that is consistent with the former, and avoids the latter."[122] Certainly, exceptionalism would explain Justice Scalia's scathing comment in the dissent, "[w]e should start calling this law SCOTUScare."[123]

Health-care data protection exceptionalism has had a far more consistent history, and HIPAA still stands tall when compared to protections given to personal data in other sectors. This exceptional protection is of great importance. Outside of health care, there is no history or expectation of strong data protection in the U.S. Of course, there are other protected sectors, but the level of data protection is relatively low or prefers data-custodian-favoring choice architectures such as opt-out. Outside of health care, the mantras of "get over it,"[124] self-regulation, and market solutions have gained more traction. The health data protection model has a far stronger baseline that resists the arguments of privacy defeatists.

The story of exceptional health-care data protection has one additional implication: the relative isolation of health-care data protection from general data protection. Health-care lawyers may not be to blame here. After all, HIPAA's

119. 132 S. Ct. 2566 (2012). *See generally* Abigail R. Moncrieff, *Understanding the Failure of Healthcare Exceptionalism in the Supreme Court's Obamacare Decision*, 142 CHEST 559, 559–60 (2012).

120. *See generally* Cass R. Sunstein, *Chevron Step Zero*, 92 VA. L. REV. 187 (2006).

121. 135 S. Ct. 2480, 2489 (2015).

122. *Id.* at 2496.

123. *Id.* at 2507.

124. Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED (Jan. 26, 1999), http://archive.wired.com/politics/law/news/1999/01/17538 [https://perma.cc/L4DD-JXHH].

"more stringent than" cooperative preemption model accepts that HIPAA provides a privacy and security floor permitting federal law's deferral to some state laws.[125] Further, health privacy policymakers have recognized that HIPAA's downstream models normatively are not the end of the line, recognizing that health-care entities also should conduct themselves by reference to FIPPS.[126] If anything, the difficulty is that health-care data protection issues have been shunned by those outside the field. HIPAA seems to be viewed as *sui generis* and health-care data protection as "solved." For example, two reports issued in 2012 by the White House and the FTC excluded health-care data from their data protection proposals.[127] However, this situation may be turning around. For instance, in its 2014 *Data Brokers* report, the FTC included the health domain in its study, even making a specific legislative recommendation to acquire the express consent of data subjects before adding health-care data.[128] Looking forward, general data protection should learn from health care's experience in dealing with downstream protective models. Similarly, policymakers revisiting health-care data protection need to accept that many of its issues cannot be handled by older models such as HIPAA or common law confidentiality.

1. History of Exceptionalism

Neither historically nor in modern law has the action for breach of confidence been unique to health-care relationships. Notwithstanding this fact, actions involving physicians are disproportionately represented in the confidence jurisprudence and the physician-patient fiduciary relationship seems to have been a powerful rationale upon which the various doctrinal bases have rested. Consider, for example, some of the very earliest breach of confidence cases that based the action (too early to call it a tort) on positive duties imposed by medical licensure statutes.[129] Later cases would

> [R]ely on various sources of public policy favoring the confidentiality of communications between a physician and a patient, including state licensing or testimonial privilege statutes, or the Principles of Medical Ethics of the American Medical Association (1957), Section 9, or the Oath of Hippocrates. Some note that while public policy considerations

125. 45 C.F.R. § 160.203(b) (2016).

126. Letter from Paul Tang, Vice Chair, HIT Policy Comm., to Dr. David Blumenthal, Nat'l Coordinator, Health Info. Tech. at 2–3 (Sept. 1, 2010), http://www.healthit.gov/sites/faca/files/hitpc_transmittal_p_s_tt_9_1_10_0.pdf [https://perma.cc/22ZW-UXNM].

127. *Framework for Protecting Privacy*, *supra* note 18, at 38; *Protecting Consumer Privacy*, *supra* note 40, at i-v.

128. *Data Brokers*, *supra* note 3 at 52.

129. *See, e.g.*, Simonsen v. Swenson, 177 N.W. 831, 832 (Neb. 1920); *see also* Smith v. Driscoll, 162 P. 572 (Wash. 1917).

> are a sound enough basis to support liability, a more appropriate basis can be found in the nature of the physician-patient relationship itself, either because of its fiduciary character or because it is customarily understood to carry an obligation of secrecy and confidence.[130]

Today, breach of confidence is recognized as a tort of general applicability.[131] However, just as its genesis depended on health-care-specific doctrines, so its primary usage remains in the health-care domain. Indeed, the tort can lay claim to being the first exceptional protection of health-care data.

In 1999, representing physician organizations, Dr. Richard Harding testified before the House of Representatives and argued, "[i]t is critically important to recognize the difference between medical records privacy and financial privacy" because "damages from breaches of medical records privacy are of a different nature."[132] This he ascribed to the extremely sensitive nature of the information contained therein, "heart disease, terminal illness, domestic violence, and other women's health issues, psychiatric treatment, alcoholism and drug abuse, sexually transmitted diseases and even adultery" that, if disclosed "can jeopardize our careers, our friendships, and even our marriages."[133]

The well-respected Institute of Medicine has long endorsed exceptionalism:

> For the most part, privacy law in [the United States] has been formulated under the assumption that holders of information about people may generally do with it what they please, constrained only by corporate ethics and the good taste of business, societal acceptance (or outrage), occasional attention by the government, pressures of consumer activist groups, and the consequences of legal actions brought by individuals or consumer groups. This historical view may prove inappropriate or even dangerous in regard to health data.[134]

Of course, the ultimate proof of exceptionalism is almost two decades of HIPAA itself and the simple fact that the largest industry in the United States is subject to the country's most comprehensive, if flawed, data protection regulation and enforcement. Although disliked by powerful health-care interests,[135] HIPAA has not faced any significant challenges. When President George W. Bush came into office, the HIPAA Privacy rule had only just been issued by Donna Shalala,

---

130. Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 523 (Ohio 1999).

131. *Id.*

132. Financial Services Act of 1999, H.R. 10, 106th Cong. § 351 (1999) (addressing the confidentiality of health and medical information).

133. *Id.*

134. HEALTH DATA IN THE INFORMATION AGE, *supra* note 2, at 191.

135. *See, e.g.*, Robert Pear, *New Privacy Rules Are Challenged*, N.Y. TIMES (Dec. 21, 2000), http://www.nytimes.com/2000/12/21/us/new-privacy-rules-are-challenged.html [https://perma.cc/F85D-YQPH].

President Clinton's HHS Secretary.[136] Incoming Secretary Tommy Thompson promised a thorough rethinking of the rule.[137] Yet only minor tweaks were made,[138] and the secretary soon announced, "President Bush wants strong patient privacy protections put in place now. Therefore, we will immediately begin the process of implementing the patient privacy rule that will give patients greater access to their own medical records and more control over how their personal information is used."[139] In 2009, the bipartisan HITECH Act strengthened HIPAA privacy, broadened its scope to directly regulate "Business Associates," and included authority to issue a health-care data breach notice (recall that Congress has not been able to pass one of general applicability).

2. Health Subdomain Exceptionalism

Obviously, general health-care data are exceptionally protected. However, a few of its subdomains exhibit additional levels of exceptionalism.[140] One of these is actually provided for in the HIPAA Privacy Rule. Process notes taken by psychotherapists are personal notes and "typically are not required or useful for treatment, payment, or health care operations purposes, other than by the mental health professional who created the notes."[141] As a result, the Privacy Rule therefore applies exceptional restrictions on patient access and health-care provider disclosure.[142]

Moving outside of HIPAA, several subdomains exhibit enhanced

136. Beth Wilson, *Clinton Issues Health Privacy Rules*, AMARILLO GLOBE-NEWS (Dec. 21, 2000), http://amarillo.com/stories/2000/12/21/usn_clintonissues.shtml#.VfBV47SRq-I [https://perma.cc/25GU-D98A].

137. *HHS Moves to Implement and Modify HIPAA Privacy Rules*, AUNTMINNIE.COM (Apr. 12, 2001), http://www.auntminnie.com/index.aspx?sec=ser&sub=def&pag=dis&ItemID=50551 [https://perma.cc/8JQY-RCTX].

138. For example, replacing the original requirement of consent, *see* 45 C.F.R. § 164.506(a), with a privacy notice, *see id.* § 164.506(b)(1) (2016).

139. Press Release, U.S. Dep't Health & Hum. Servs., Statement by Tommy G. Thompson, Secretary Department of Health and Human Services (Apr. 12, 2001), http://archive.hhs.gov/news/press/2001pres/20010412.html [https://perma.cc/G34Y-E3MS].

140. The list of examples that follow is not closed. For example, Stacey Tovino has floated neuroimaging exceptionalism. Stacey A. Tovino, *Functional Neuroimaging Information: A Case for Neuro Exceptionalism?*, 34 FLA. ST. U. L. REV. 415, 485 (2007). Further, Mark Rothstein has discussed the possibility for epigenetic exceptionalism. Mark A. Rothstein, *Epigenetic Exceptionalism*, 41 J.L. MED. & ETHICS 733, 735; *see also* Nicolas P. Terry, *Developments in Genetic and Epigenetic Data Protection in Behavioral and Mental Health Spaces*, 33 BEHAV. SCI. & L. 653 (2015). Finally, some states have safe harbor rules that protect physicians who are diverted to physician health programs in the case of mental health or substance use disorders. *See generally* J. Wesley Boyd & John R. Knight, *Ethical and Managerial Considerations Regarding State Physician Health Programs*, 6 J. ADDICT. MED. 243 (2012).

141. *HIPAA Privacy Rule and Sharing Information Related to Mental Health*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/mhguidance.html [https://perma.cc/U8CU-QW4M].

142. 45 C.F.R. § 164.501 (2016).

exceptionalism. HIV-AIDS is treated exceptionally compared to other STDs.[143] Generally-applicable federal law, such as the Rehabilitation Act[144] and the Americans with Disabilities Act, apply to claims of discrimination.[145] And, of course, HIPAA applies a data protection baseline.[146] However, state laws tend to provide additional, exceptional data protection such as anonymous testing and heightened controls on disclosure.[147]

GINA utilizes two models of data protection. First, GINA prohibits downstream point of use discrimination by employers (Title I) and health insurers (Title II). However, GINA also prohibits the requiring or (in many cases) acquiring of genetic information. This is an upstream collection model of protection and has resulted in large settlements with the EEOC in cases dealing with unlawful requests for family medical histories[148] and a landmark $2.2 million jury verdict in the recent "devious defecator" case.[149]

Less well-known are the Substance Abuse Confidentiality Regulations (often referred to by their citation, "45 C.F.R. Part 2") promulgated by HHS's Substance Abuse and Mental Health Services Administration (SAMSHA).[150] These regulations subject federally-assisted programs that maintain alcohol and drug abuse patient records to downstream disclosure restrictions that are considerably more stringent than those found in HIPAA. There is also a complex web of overlapping state mental health and substance abuse laws that further complicate the picture.[151] Recently, 45 C.F.R. Part 2 has attracted considerable attention because of Congressional concerns over the information–sharing costs

143. *See, e.g.*, CAL. HEALTH & SAFETY CODE § 120990 (West 2017); MICH. COMP. LAWS ANN. § 333.5133 (West 2011). *Cf.* MONT. CODE ANN. § 50-16-1014 (West 2016).

144. Rehabilitation Act of 1990 § 504, 42 U.S.C. § 12101 (2012).

145. *See* Bragdon v. Abbott, 524 U.S. 624 (1998).

146. *See Health Information Privacy Enforcement Examples Involving HIV/AIDS*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/ocr/civilrights/activities/examples/AIDS/hiphiv/aidscases.html [https://perma.cc/3RFM-YBBF].

147. *See, e.g.*, N.Y. PUB. HEALTH LAW ch. 45, art. 27-F (McKinney 2016); *see generally* Roger Doughty, Comment, *The Confidentiality of HIV-Related Information: Responding to the Resurgence of Aggressive Public Health Interventions in the Aids Epidemic*, 82 CAL. L. REV. 111 (1994).

148. *See, e.g.*, Press Release, U.S. Equal Employment Opportunity Comm'n, Founders Pavilion Will Pay $370,000 to Settle EEOC Genetic Information Discrimination Lawsuit (Jan. 13, 2014), http://www.eeoc.gov/eeoc/newsroom/release/1-13-14.cfm [https://perma.cc/K9EX-QXAM].

149. *Georgia Workers Win $2.2 Mln in 'Devious Defecator' Case*, REUTERS (June 23, 2015), http://www.reuters.com/article/verdict-dna-defecator-idUSL1N0Z916520150623 [https://perma.cc/7ZAY-Y8V4].

150. Promulgated under the Drug Abuse Prevention, Treatment, and Rehabilitation Act § 408, 42 U.S.C. § 290ee-3 (2012).

151. *See generally* RTI INTERNATIONAL, BEHAVIORAL HEALTH DATA EXCHANGE CONSORTIUM: ONC STATE HEALTH POLICY CONSORTIUM PROJECT FINAL REPORT (June 2014), https://www.healthit.gov/sites/default/files/bhdeconsortiumfinalreport_06182014_508_compliant.pdf [https://perma.cc/ZHA2-NKSF].

it imposes.[152] For example, in a letter to a Congressional committee supportive of the 21st Century Cures Act the Patient Safety Movement urged, "[a]t a minimum, this problem should be addressed by streamlining the consent process for the sharing of medical records in integrated care settings."[153] Reform of Part 2 has also been targeted in Congressman Tim Murphy's Helping Families in Mental Health Crisis Act of 2016,[154] creating concern among some privacy advocates.[155] In January 2017, SAMSHA published a rule that allows a broad "to whom" consent that it believes will increase the sharing of substance use records through EHRs and Health Information Exchanges. The rule also permits health-care data custodians to share substance abuse data with researchers.[156]

IV. TURBULENCE, DISRUPTION, AND ARBITRAGE IN PRACTICE

A. Professional Health-Care Domain vs. Consumer Domain

In the words of a recent report by the HIT Policy Committee (HITPC), a federal advisory committee established by the HITECH Act,[157] "[m]uch of the health-related information generated today is not regulated by [HIPAA,]"[158] and "[t]he exact same health-related information is regulated differently based on the entity processing the information."[159] As already discussed, the prerequisite for regulatory turbulence, disruption, and potentially arbitrage is the existence of differential regulatory models. For the purposes of the present analysis, two

152. *See generally* Michelle Andrews, *Debate Arises Over HHS Plans For Privacy Rules On Addiction Treatment*, KAISER HEALTH NEWS (Mar. 22, 2016), http://khn.org/news/debate-arises-over-hhs-plans-for-privacy-rules-on-addiction-treatment [https://perma.cc/XD7T-CYG6].

153. Letter from Jim Bialick, President, Patient Safety Movement Foundation, to Fred Upton, Chairman, Energy & Commerce Committee, and Frank Pallone, Ranking Member, Energy & Commerce Committee (Aug. 19, 2015), http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/114/Letters/hr6/PSMF.pdf [https://perma.cc/J55G-5N5V].

154. Helping Families in Mental Health Crisis Act of 2016, H.R. 2646, 114th Cong. (as passed by House, Jul. 6, 2015).

155. *See, e.g.*, Kimberly Leonard, *Would Mental Health Laws Threaten Privacy and Patients' Rights?*, U.S. NEWS & WORLD REPORT (Aug. 12, 2015), http://www.usnews.com/news/articles/2015/08/12/patients-rights-privacy-concerns-highlighted-in-mental-health-laws [https://perma.cc/9DEB-9C6E]; Peter Sullivan, *Dems Introduce Alternative to GOP's Mental Health Bill*, THE HILL (Feb. 2, 2016), http://thehill.com/policy/healthcare/267868-dems-introduce-alternative-to-gop-led-mental-health-bill [https://perma.cc/SW23-NKT6].

156. Confidentiality of Substance Use Disorder Patient Records, 82 Fed. Reg. 6052 (Jan. 18, 2017) (to be codified at 42 C.F.R. pt. 2).

157. HITECH Act § 3002, 42 U.S.C. 300jj-12 (2012).

158. *Health Big Data Recommendations*, HEALTH IT POL'Y COMMITTEE PRIVACY & SECURITY WORKGROUP, 4 (Aug. 2015), http://www.healthit.gov/facas/sites/faca/files/HITPC_Draft_PSWG_Big_Data_Transmittal_2015-08-11.pdf [https://perma.cc/8NL4-V9BT] [hereinafter *Health Big data Recommendations*].

159. *Id.* at 11.

regulatory domains are posited: first, a *professional* health-care domain and second, a *consumer* health-care domain.

The professional domain is heavily populated with regulatory models. For example, it is home to state regulation of health-care providers, custom-based quality and safety, medical malpractice doctrine, the federal regulation of prescription drugs and medical devices, state and federal regulation of professional data curators (HIPAA data custodians), unique "fraud and abuse" transactional regulations, specialized antitrust scrutiny, and institutional review board/Common Rule scrutiny of human subjects research. Befitting the country's most regulated industry, there are considerably more examples that could be cited.

In contrast, the *consumer* health-care domain is larger, yet both less regulated and considerably more indeterminate. For example, OTC pharmaceuticals are only lightly regulated by FDA,[160] a few issues regarding consumer platforms may attract some FCC scrutiny, common law products liability or the Consumer Product and Safety Act may apply to a narrow range of safety issues, and mobile apps and wearables are either unregulated or currently benefiting from FDA discretion. Meanwhile, some parts of the domain, crowdsourcing research models, for example, are barely regulated. Others, such as data-curation by data subjects, seem very hard to regulate.

Parallel, and potentially exacerbating, regulatory disruptions can occur at the process level when different regulatory agencies operate in different domains. For example, HHS's Office for Civil Rights (HHS-OCR) regulates professional domain data protection but FTC regulates consumer space. Similarly, FDA regulates medical devices but the Consumer Product Safety Commission or the FCC might deal with the consumer domain. A further complication may be overlapping state and federal laws (e.g., state products liability law overlapping with FDA or state law or health-care data protection legislation overlapping with HIPAA privacy or security).

Differentiated regulatory domains can tolerate *some* turbulence. Further, not all turbulence develops into disruption. Consider the following episodes of turbulence between professional and consumer domain. First, Google Glass: Google introduced (initially only to "Glass Explorers") this augmented reality wearable in 2013. It was designed and sold as a consumer product.[161] Increasingly, doctors joined the ranks of the "explorers" and soon Glass appeared

160. *See Drug Applications for Over-the-Counter (OTC) Drugs*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/drugs/developmentapprovalprocess/howdrugsaredevelopedandapproved/approvalapplications/over-the-counterdrugs/default.htm [https://perma.cc/V33W-4JHU].

161. Vidya Viswanathan, *Is There a Place for Google Glass in Hospitals?*, ATLANTIC (July 21 2014), www.theatlantic.com/health/archive/2014/07/is-there-a-place-for-google-glass-in-hospitals/374153/ [https://perma.cc/BF27-85YZ].

in hospitals, used during surgeries, for EHR access and training.[162] The problem was that while Glass satisfied the minimal regulatory standards of the consumer domain, it caused regulatory problems in the professional domain. For example, it was not HIPAA-compliant, in some implementations it came close to FDA regulated device territory, and its "stealth" camera tempted marginal collection of health and personal data.[163] Before Glass could become an example of full-on regulatory disruption, Google announced it would cease selling the device.[164]

23andMe, a consumer-facing DNA test kit and analytic service, was launched in 2007.[165] The product's marketing stated that the kits provided health reports on multiple diseases and conditions, written with enough specificity to prompt FDA inquiry. 23andMe featured genotyping, not sequencing (although those technologies are beginning to merge). Notwithstanding that distinction, here was an example of professional DNA testing migrating into the consumer health domain.[166] Apparently, FDA spent four years trying to work with 23andMe before sending the archetypal warning letter informing the company it was selling an unapproved medical device contrary to the Food, Drug and Cosmetic Act.[167] As George Annas and Sherman Elias later noted, "[c]linicians will be central to helping consumer–patients use genomic information to make health decisions."[168] As a result they argued, "[a]ny regulatory regime must recognize this reality by doing more than simply adding the tagline on most consumer ads for prescription drugs: 'Ask your physician.'"[169] When *23andMe* finally had to confront the FDA's concerns, it decided to stop marketing the kit

162. Vala Afshar, *How Google Glass Will Transform Healthcare*, HUFFINGTON POST (Oct. 17, 2014), http://www.huffingtonpost.com/vala-afshar/how-google-glass-will-tra_b_6003100.html [https://perma.cc/FLE6-EX5V]; Helen Gregg, *5 Hospitals Using, Piloting Google Glass*, BECKER'S HEALTHCARE (Mar. 18, 2014), http://www.beckershospitalreview.com/healthcare-information-technology/5-hospitals-using-piloting-google-glass.html [https://perma.cc/R8T3-8RD8].

163. *See generally* Nicolas P. Terry, Chad S. Priest & Paul P. Szotek, *Google Glass and Health Care: Initial Legal and Ethical Questions*, 8 J. HEALTH & LIFE SCI. L. 93 (2015).

164. Jim Edwards, *Google Ends Sales of Google Glass*, BUSINESS INSIDER (Jan. 16, 2015), http://www.businessinsider.com/google-ends-sales-of-google-glass-2015-1 [https://perma.cc/V8ZM-7C6F].

165. Lisa Baertlein, *Google-Backed 23andMe Offers $999 DNA Test*, USA TODAY (Nov. 20, 2007), http://usatoday30.usatoday.com/tech/webguide/internetlife/2007-11-20-23andme-launch_N.htm [https://perma.cc/K4SC-A7XY].

166. *See, e.g.*, Robert J. Elshire et al., *A Robust, Simple Genotyping-by-Sequencing (GBS) Approach for High Diversity Species*, 6 PLOS ONE e19379 (2011).

167. Letter from Alberto Gutierrez, Director, Office of In vitro Diagnostics and Radiological Health, to Ann Wojcicki, CEO, 23andMe, Inc. (Nov. 22, 2013), http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2013/ucm376296.htm [https://perma.cc/SE8F-5C8U]; *see generally* Matthew Herper, *23andStupid: Is 23andMe Self-Destructing?*, FORBES (Nov. 25, 2013), http://www.forbes.com/sites/matthewherper/2013/11/25/23andstupid-is-23andme-self-destructing/ [https://perma.cc/WM3Q-WDQK].

168. George J. Annas & Sherman Elias, *23andMe and the FDA*, 370 NEW ENG. J. MED. 985, 987 (2014).

169. *Id.*

as a diagnostic tool and changed its reports to generic information rather than anything approaching diagnostics.[170] Subsequently, FDA approved the company's marketing of more narrowly focused tests for Bloom syndrome[171] and autosomal recessive disorders.[172] Furthermore, the FDA designation of the tests as over-the-counter[173] led to the obviation of some state law limitations on the services, making them available across the country.[174]

23andMe was a private initiative at first avoiding and subsequently seeking regulatory approval. In contrast, the "Blue Button"[175] is a federal government initiative permitting Medicare beneficiaries[176] and VA patients[177] to transfer their health records. Users may download the data in text, PDF, or Blue Button formats. The Office of the National Coordinator (ONC) and the Centers for Medicare & Medicaid Services (CMS) are targeting similar models as a way of increasing patient engagement and data liquidity in Stages 2 and 3 of Meaningful Use.[178]

---

170. Brian Fung, *Bowing Again to the FDA, 23andMe Stops Issuing Health-related Genetic Reports*, WASH. POST (Dec. 6, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/12/06/bowing-again-to-the-fda-23andme-stops-issuing-health-related-genetic-reports [https://perma.cc/UT4M-ZLC7].

171. Press Release, U.S. Food & Drug Admin., FDA Permits Marketing of First Direct-to-Consumer Genetic Carrier Test for Bloom Syndrome (Feb. 19, 2015), http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/UCM435003 [https://perma.cc/XAV7-8FSA].

172. Andrew Pollack, *23andMe Will Resume Giving Users Health Data*, N.Y. TIMES (Oct. 21, 2015), http://www.nytimes.com/2015/10/21/business/23andme-will-resume-giving-users-health-data.html [https://perma.cc/JP2T-26CU]. FDA continues to investigate other direct-consumer genetic tests. *See, e.g.*, Letter from James L. Woods, Deputy Director Patient Safety and Product Quality, Office of In Vitro Diagnostics and Radiological Health, to Rajasingam S. Jeyendran, DNA-Cardiocheck, Inc. (Nov. 2, 2015), http://www.fda.gov/downloads/MedicalDevices/ResourcesforYou/Industry/UCM471784.pdf [https://perma.cc/Q4NP-84JK].

173. Letter from Courtney H. Lias, Director, Division of Chemistry and Toxicology Devices, Office of In Vitro Diagnostics and Radiological Health, to Kathy Hibbs, Chief Legal and Regulatory Officer, 23andMe, Inc. (Oct. 1, 2015), http://www.accessdata.fda.gov/cdrh_docs/pdf14/den140044.pdf [https://perma.cc/A86T-7JWU].

174. Press Release, 23andMe, 23andMe Genetic Service Now Fully Accessible to Customers in New York and Maryland (Dec. 4, 2015), http://mediacenter.23andme.com/?p=2084 [https://perma.cc/RMG4-FERN].

175. *About Blue Button*, HEALTHIT.GOV, http://www.healthit.gov/patients-families/blue-button/about-blue-button [https://perma.cc/G8C5-626J].

176. *Download Claims with Medicare's Blue Button*, CTRS. FOR MEDICARE & MEDICAID SERVS., https://www.medicare.gov/manage-your-health/blue-button/medicare-blue-button.html [https://perma.cc/44LQ-SKGV].

177. *The My HealtheVet Community*, U.S. DEP'T VETERANS AFF., https://www.myhealth.va.gov/mhv-portal-web/mhv-community [https://perma.cc/G2GZ-7L7L].

178. Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Stage 2, 77 Fed. Reg. 53,968, 53,973 (Sept. 4, 2012) (to be codified at 42 C.F.R. pts. 412, 413, and 495). For more detail see *Eligible Professional, Meaningful Use Core Measures, Measure 7 of 17, Stage*, CTRS. FOR MEDICARE & MEDICAID SERVS. 2 (Aug. 2014), https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/Stage2_EPCore_7_PatientElectronicAccess.pdf [https://perma.cc/E5XM-MRHR].

What do we learn from these three examples of regulatory turbulence? Both Google Glass and *23andMe* were temporary phenomena. The former was a consumer domain product that caused some turbulence in the professional space but which was withdrawn from the market before disruption could occur (or HIPAA indeterminacy or FDA device regulation issues were resolved). The latter was the inverse; a professional domain technology sold into consumer space. *23andMe* likely was subject to professional domain medical device regulation. It caused turbulence at a process level because its developer seemingly was oblivious to or unmindful of FDA regulations. As a result, for several years there was accidental disruption until regulator-regulatee information costs equalized. Once *23andMe* was forced to confront the FDA's concerns, it decided to stop marketing the kit as diagnostic.

Only the last of these three examples exhibits a transition from turbulence to disruption. The entirely well meaning, patient-autonomy-respecting Blue Button program has a seriously disruptive effect. It takes HIPAA-protected data and, with a single click from the data subject, moves it into an almost completely unprotected domain. This is a model now being repeated by Stage 3 of Meaningful Use, which adds the option of an application programming interface (API) linkage between a provider's EHR and a patient's app.[179] It could be argued that there is simply no data protection issue when the data subject holds the data. However, the data likely implicates persons other than the data subject (such as the subject's family members) and so any data compromise is neither benign nor intrinsically limited. Further, there is disruption in fact and substantial potential for confusion when the "same" data are subject to both professional domain regulation (professional curation) and consumer domain-regulation-lite (personal curation). Clicking the Blue Button strips data protection from clinical data. Major questions arise as to how to adequately warn the data subject at the point of conversion and whether policymakers can appropriately remodel data subjects' expectations and responsibilities.

B. Example One: Big Data

Observations as to either the sectoral limitations of U.S. data protection or the rise of commercial data brokers are hardly novel. A decade ago, Dan Solove and Chris Hoofnagle noted, "[a]lthough most industrialized nations have comprehensive data protection laws, the United States has maintained a sectoral approach where certain industries are covered and others are not. In particular, emerging companies known as 'commercial data brokers' have frequently

179. Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Stage 3 and Modifications to Meaningful Use in 2015 Through 2017, 80 Fed. Reg. 62,762 (Oct. 16, 2015); 42 C.F.R. § 495.24 (2016).

slipped through the cracks of U.S. privacy law."[180] Solove and Hoofnagle did not use the terms disruption or arbitrage but probably had something similar in mind when stating, "[m]any companies brokering in data have found ways to avoid being regulated by [FCRA]."[181] More recently, Kate Crawford and Jason Schultz observed, "[n]ot only does Big Data's use have the potential to circumvent existing antidiscrimination regulations, but it may also lead to privacy breaches in health care . . ."[182]

As reported by FTC:

> [D]ata brokers. . . purchase information about individuals from wide-ranging commercial sources. For example, the data brokers obtain detailed, transaction-specific data about purchases from retailers and catalog companies. Such information can include the types of purchases (e.g., high-end shoes, natural food, toothpaste, items related to disabilities or orthopedic conditions), the dollar amount of the purchase, the date of the purchase, and the type of payment used.[183]

In most cases, data brokers will not find dealing directly with HIPAA covered entities (or their business associates) to be a good source of clinical data. Generally, HIPAA entities would be unable to supply clinical data without data subject (patient) authorization,[184] a heightened form of consent. Or, if HIPAA entities agree to the broker's request for a "limited data set," the disclosure would be restricted to "research" only processing and subject to a re-identification-limiting data use agreement.[185]

Denied access to most of the health-care "deep web,"[186] data brokers therefore construct clinical data "proxies" from other data pools. These pools, like the public records and other databases they mine, exist outside of HIPAA-protected space. They do not completely ignore data that has been subject to HIPAA protection. For example, they may acquire de-identified data; HIPAA data that have been de-identified are no longer subject to HIPAA.[187] They may also acquire HIPAA data that have been legally shared with public health authorities,[188] who subsequently made anonymized or de-identified data sets

180. Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 357 (2006).

181. *Id.* at 359.

182. Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward A Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 99 (2014).

183. *Data Brokers*, *supra* note 3, at 13.

184. 45 C.F.R. § 164.508 (2016).

185. 45 C.F.R. § 164.514 (2016).

186. *See generally* Jose Pagliery, *The Deep Web You Don't Know About*, CNN (Mar. 10, 2014), http://money.cnn.com/2014/03/10/technology/deep-web/index.html [https://perma.cc/DJP9-4YG9].

187. *See supra* text accompanying note 90 *et seq.*

188. 45 C.F.R. § 164.512(b) (2016).

available.[189]

As discussed elsewhere,[190] these data are supplemented by medical-inflected data, what McKinsey refers to as "[p]atient behavior and sentiment data that describe patient activities and preferences, both inside and outside the healthcare context."[191] These data are culled from social media interactions, retail stores, web trackers, online transactions, mobile phone location trackers, fitness wearables, and so on. Data brokers subsequently leverage their sophisticated algorithms and the breadth of their triangulation databases to re-identify the data.[192]

Increasingly, our everyday interactions will trigger unrealized or unconsented collection of data about us from Internet of Things devices, including our location and physical, even medical, condition. As pointed out by Elizabeth Pike, another likely data pool is the "non-consensual collection and use of genetic material."[193] Pike identifies regulatory disruption because "[i]n many ways, commercial endeavors are less heavily regulated than federally funded research endeavors outside the Common Rule's reach. And commercial entities are unlikely to be "covered entities" subject to HIPAA's Privacy Rule."[194]

These disparate, essentially unregulated data pools make possible the following claim by one major data broker:

> We have one of the largest and most comprehensive collections of healthcare information in the world, spanning sales, prescription and promotional data, medical claims, electronic medical records and social media. Our scaled and growing data set, containing over 10 petabytes of unique data, includes over 85% of the world's prescriptions by sales revenue and approximately 400 million comprehensive, longitudinal, anonymous patient records. We standardize, organize, structure and integrate this data by applying our sophisticated analytics and leveraging our global technology infrastructure to help our clients run their organizations more efficiently and make better decisions to improve their operational and financial performance.[195]

---

189. *See, e.g.*, Sean Hooley & Latanya Sweeney, *Survey Of Publicly Available State Health Databases*, HARV. U. 3 (2013), http://dataprivacylab.org/projects/50states/1075-1.pdf [https://perma.cc/P8KE-2NDK].

190. *See* Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65, 84–87 (2014).

191. Peter Groves et al., *The 'Big Data' Revolution in Healthcare*, MCKINSEY & CO. 3 (Jan. 2013), http://www.pharmatalents.es/assets/files/Big_Data_Revolution.pdf [https://perma.cc/RG3E-2JQ5].

192. *See generally* Terry, *supra* note 140.

193. Elizabeth R. Pike, *Securing Sequences: Ensuring Adequate Protections for Genetic Samples in the Age of Big Data*, 37 CARDOZO L. REV. 1977, 1980 (2015).

194. *Id.* at 2007 (references omitted).

195. *Registration Statement under the Securities Act of 1933 (Form S-1)*, IMS HEALTH

The regulatory disruption is clear and arbitrage highly likely. Data brokers, generally shut out of protected health-care data, are able to create proxies for those data in a lightly regulated HIPAA-free zone. Crawford and Schultz go further, noting that the "predictive privacy harms" caused by big data are such that traditional upstream and downstream data protection models ("collection, processing and disclosure") can be circumvented.[196]

Medically inflected data collected from, say, social media, apps, and retail stores can quickly result in highly targeted advertising. The predictive analytics at the root of big data "learns from experience (data) to predict the future behavior of individuals in order to drive better decisions."[197] *Smith v. Facebook, Inc.*,[198] a recently filed class action against the social media company and various health-care providers offers insight into how such systems work. According to the complaint, the web sites of various health-care providers include "referrer" headers and third-party tracking "cookies" that allow Facebook to link search requests (e.g., stomach cancer diagnosis) to its own users. These search requests, coupled with other data such as "like" activity, allegedly enabled Facebook to create health-related profiles of its users against which it could sell health-related advertising specifically targeted at them. Indeed, the world's largest social media platform collects ninety-eight personal data points about their users for the purpose of targeting advertising.[199] These include all manner of personal and financial information, including parental status and whether pregnant.[200]

Increasingly, health scoring and other data segmentation carries the threat of discrimination. At first sight, wellness firms that mine data about employees and then "nudge" them into healthier pursuits seem relatively benign. However, there are considerable risks of these data being exposed to employers or their aggregate nature being undermined by small populations, enabling identification.[201]

Health data acquired by data brokers can also be looped back into the health-care space for discriminatory purposes. As is well known, the ACA prohibits pre-

---

HOLDINGS, INC. (Jan. 2, 2014), http://www.sec.gov/Archives/edgar/data/1595262/000119312514000659/d628679ds1.htm [https://perma.cc/G385-EFVF].

196. Crawford & Schultz, *supra* note 182, at 106.

197. ERIC SIEGEL, PREDICTIVE ANALYTICS: THE POWER TO PREDICT WHO WILL CLICK, BUY, LIE, OR DIE 11 (2013).

198. Complaint, Smith v. Facebook, Inc., 2016 WL 1042966 (N.D.Cal.) (5:16-cv-01282) (filed Mar. 15, 2016).

199. Caitlin Dewey, *98 Personal Data Points That Facebook Uses to Target Ads to You*, WASH. POST, (Aug. 19, 2016), https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/ [https://perma.cc/75Y9-APB5].

200. *Id.*

201. *See* Rachel Emma Silverman, *Bosses Tap Outside Firms to Predict Which Workers Might Get Sick*, WALL ST. J. (Feb. 17, 2016), http://www.wsj.com/articles/bosses-harness-big-data-to-predict-which-workers-might-get-sick-1455664940 [https://perma.cc/WFM3-RPFF]; Valentina Zarya, *Employers Are Quietly Using Big Data to Track Employee Pregnancies*, FORTUNE (Feb. 17, 2016), http://fortune.com/2016/02/17/castlight-pregnancy-data [https://perma.cc/W88H-CV3N].

existing condition exclusions, discriminatory premium rates, and generally requires guaranteed issue.[202] Guaranteed issue and related regulations generally do not apply to life insurers who are customers for big data proxies. Even more troubling are reports of health insurers who use data-mined prescription drug data to continue their discrimination against high cost patients.[203] For example, big data analytics permit insurers to predict the health conditions of those in their risk pools. They could then move drugs associated with patients with expensive chronic conditions to high cost-sharing tiers in the hope of discouraging those patients from applying for coverage.[204] As a result, unregulated big data has the potential to frustrate some of the mainstay policies of our health-care system.

C. Example Two: Mobile Health Data

The defining characteristic of mobile health is that it is patient-facing. Unlike most examples of digital health, patients or pre-patients interact directly with mobile health hardware and software, frequently without the direct involvement of conventional health-care providers. Most of these relationships form and interactions occur in a consumer rather than a professional space. As a result, serious turbulence, even regulatory disruption, can occur. In some ways, emerging mobile health-care services mirror the Uber-Lyft model. Like those car services, mobile health steps around bureaucracy-laden incumbents that have been slow to adopt information technologies, reform their guilds, modernize their financing, or offer coherent alternatives to inconvenient centralized locations.

Consequently, mobile health, a combination of mobile health apps, wearable devices, and the rapidly iterating Internet of Health Things, suggest some health-care business disruption. Specifically, mobile health promises personalized care, improved convenience, and lower cost.

Of course, the HIPAA privacy and security rules apply to traditional health-care providers such as doctors and hospitals. Therefore, if a hospital or health insurer (or a business associate) builds a patient portal app to provide access to EHR or claims information, HIPAA likely applies. However, the vast majority of health apps are not curated, sold or implemented by HIPAA "covered entities"; they are built by technology companies and sold through app stores. As a result,

202. Patient Protection and Affordable Care Act of 2010, Pub. L. No. 111-148, § 1201, 124 Stat. 119, 154–61 (2010).

203. *See, e.g.*, Jordan Robertson, *The Pitfalls of Health-Care Companies' Addiction to Big Data*, BNA BLOOMBERG HEALTH IT L. & INDUSTRY REP. (Sept. 23, 2015), http://news.bna.com/hiln/HILNWB/split_display.adp?fedfid=76390826&vname=hitrbulallissues&jd=a0h3f2f8b0&split=0 [https://perma.cc/DQL6-2YB4].

204. Douglas B. Jacobs & Benjamin D. Sommers, *Using Drugs to Discriminate — Adverse Selection in the Insurance Marketplace*, 372 NEW ENG. J. MED. 399 (2015); *see also* Julie Appleby, *Got Insurance? You Still May Pay a Steep Price for Prescriptions*, KAISER HEALTH NEWS (Oct. 13, 2014), http://khn.org/news/got-insurance-you-still-may-pay-a-steep-price-for-prescriptions [https://perma.cc/YVX4-V73M].

much of the fitness and health data collected by mobile apps and wearables have very thin legal protection. ONC recognized this problem in a 2016 report to Congress concluding "Wearable fitness trackers, health social media, and mobile health apps are premised on the idea of consumer engagement. However, our laws and regulations have not kept pace with these new technologies."[205]

This also seems to be the case with mobile platform health data aggregators and APIs, such as those offered by Apple with its "Health" app, HealthKit SDK,[206] and "CareKit" framework.[207] Platform developers appear to take the position that their apps do not access any HIPAA-protected data but merely act as traffic cops working at the direction of the data subject. Take as an example a patient who uses a tracker to collect health data and who wants to share that with his or her health-care provider's patient portal app. The sharing is facilitated through the mobile platform health app. If that app is only opening and closing doors at the instructions of the patient then, the argument is made, the platform app is not "touching" any HIPAA data.[208]

Tens of thousands of mobile health apps are now collecting vast quantities of health-care data. However, the majority of these apps are operating in the HIPAA-free zone with little or no regulation as to how they should share data with third parties or what the security is expected of any off-device data storage. Of course, some app/wearable developers (no doubt with an eye on the growing market for "wellness" products being promoted or required by insurers and employers) are beginning to advertise HIPAA-compliance.[209]

The mobile health app space is a perfect breeding ground for regulatory disruption and arbitrage. The professional domain is highly regulated by HIPAA

---

205. *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA*, U.S. DEP'T HEALTH & HUM. SERVS. 32 (June 2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf [https://perma.cc/4JV7-8DDT] [hereinafter *Health Data Collected by Entities Not Regulated by HIPAA*].

206. *Develop Health and Fitness Apps that Work Together*, APPLE, INC., https://developer.apple.com/healthkit [https://perma.cc/7L9A-QG27].

207. Press Release, Apple, Inc., Apple Advances Health Apps with CareKit: New Software Framework Helps Developers Empower People to Take a More Active Role in their Health (Mar. 21, 2016), http://www.apple.com/pr/library/2016/03/21Apple-Advances-Health-Apps-with-CareKit.html [https://perma.cc/26SQ-NLT5].

208. *See* Mark Sullivan, *While Apple HealthKit Works out Bugs, Cleveland Clinic Uses Microsoft's HealthVault Platform to Reach Remote Patients*, VENTUREBEAT (Sept. 23, 2014), http://venturebeat.com/2014/09/23/while-apple-healthkit-works-out-bugs-cleveland-clinic-uses-microsofts-healthvault-platform-to-reach-remote-patients [https://perma.cc/KMM3-AHJU].

209. *See* Press Release, Fitbit, Inc., Fitbit Extends Corporate Wellness Offering with HIPAA Compliant Capabilities (Sept. 16, 2015), http://www.businesswire.com/news/home/20150916005371/en/#.VgAIX7SRq-I [https://perma.cc/B6FN-2EFA] ("Our compliance with HIPAA safeguards formalizes this commitment, and, more importantly, it creates opportunities for more effective relationships with corporate wellness customers." (quoting James Park, CEO and Co-Founder, Fitbit).

but the consumer domain is either unregulated or less regulated (limited to *ab initio* app store[210] or *ex post facto* FTC[211] regulation). Disruption and arbitrage in this mobile space are ongoing, as can be seen from the dysfunctional state of medical device regulation.[212] Indeed, the current regulatory status of these devices is sufficiently complicated that HHS-OCR, FTC, and FDA have felt compelled to publish an interactive tool in attempt to guide app developers through the regulatory confusion.[213]

Privacy and security issues are mounting.[214] Many medical apps have unsatisfactory data privacy policies,[215] and one recent study found "that on average 87.7% of Android devices are exposed to at least one of [eleven] known critical vulnerabilities. . ."[216] More pointedly, Huckvale and colleagues recently examined the privacy and security risks of mobile health apps that had been accredited (for clinical safety) by the English National Health Service (NHS) Health Apps Library. Overall, the study found a low level of encryption of user data at rest (on the device) or in motion and a lack of transparency in privacy policies.[217] In a 2016 report funded by the Office of the Privacy Commissioner of Canada, Hilts and colleagues documented how fitness trackers (Apple's Watch aside) emitted persistent unique identifiers that could enable tracking of users and that several also had other basic security flaws, including a failure to encrypt data in motion.[218]

---

210. *App Store Review Guidelines*, APPLE, INC., https://developer.apple.com/app-store/review/guidelines [https://perma.cc/CDB8-Q2F4].

211. *See, e.g.*, LabMD, Inc., FTC No. 102-3099 (2016), https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter [https://perma.cc/BR4S-Z6AM].

212. *See generally* Nathan Cortez, *The Mobile Health Revolution?*, 47 U.C. DAVIS L. REV. 1173 (2014).

213. *Mobile Health Apps Interactive Tool*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool [https://perma.cc/QV96-C7EH].

214. *See generally* Nicolas Terry, Hall Render Professor of Law & Executive Director, Hall Center for Law and Health, Indiana University Robert H. McKinney School of Law, Opening Remarks for House Energy and Commerce Subcommittee Hearing on Health Care Apps (July 13, 2016), http://docs.house.gov/meetings/IF/IF17/20160713/105197/HHRG-114-IF17-Wstate-TerryN-20160713.pdf [https://perma.cc/HVF2-K29J]; *Disrupter Series: Health Care Apps: Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the H. Comm. on Energy & Commerce*, 114th Cong. (Jul. 13, 2016), https://energycommerce.house.gov/hearings-and-votes/hearings/disrupter-series-health-care-apps [https://perma.cc/3T2A-XNRU].

215. Sarah R. Blenner, Melanie Köllmer, Adam J. Rouse, Nadia Daneshvar, Curry Williams & Lori B. Andrews, *Privacy Policies of Android Diabetes Apps and Sharing of Health Information*, 315 JAMA 1051 (2016).

216. Daniel R. Thomas et al., *Security Metrics for the Android Ecosystem*, U. CAMBRIDGE (Oct. 12, 2015), https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf [https://perma.cc/TG3N-LJBW].

217. Kit Huckvale et al., *Unaddressed Privacy Risks in Accredited Health and Wellness Apps: A Cross-Sectional Systematic Assessment*, 13 B.M.C. MED. 1 (2015).

218. Andrew Hilts et al., EVERY STEP YOU FAKE: A COMPARATIVE ANALYSIS OF FITNESS TRACKER PRIVACY AND SECURITY, OPEN EFFECT, (Feb. 2016), https://openeffect.ca/reports

Finally, the patient-facing, patient-data curating aspects of mobile health apps and their wearable fellow-travelers raise another, much more fundamental issue (and one not necessarily unique to health-care data). Data protection models and their implementation have been built around institutional curation of people's data and carve-outs for other institutions interested in that data. Personal or self-curation enabled by personal technologies presents an asymmetric question, whether institutions can access that data under conditions set by data subjects.[219] That question was at the root of the 2016 stand-off between Apple and the FBI over access to data encrypted on an iPhone.[220] If technology continues to outstrip regulation, an open question is whether pre-patients and patients will combat regulatory disruption by moving their data to the secure enclaves[221] they control and thereafter decide themselves if, how, and when to share data with institutions whose services they wish to engage. At one level this technological and conceptual shift will protect health-care data and reduce regulatory arbitrage. At another, however, it will cripple appropriate data sharing between patients and providers or researchers and sadly signal policymakers' inability to address the level of data protection desired by consumers.

V. DATA PROTECTION VERSUS DATA LIQUIDITY

Calls for increased data liquidity to further fuel the information society are hardly new. In the health-care domain, they frequently translate into public goods arguments. Further, in the traditional health-care space, there are some critically important policy initiatives that often are cast as at odds with existing HIPAA protections, let alone any increased upstream data protection. Currently, these include clinical interoperability and medical research.

A. Clinical Interoperability

Interoperability began with a plan announced by President Bush in 2004 "to ensure that most Americans have electronic health records within the next 10 years."[222] Moving from paper to electronic records merely substitutes electronic

/Every_Step_You_Fake.pdf [https://perma.cc/AUQ4-D74U].

219. *See generally* Adrian Groper, *Apple and the 3 Kinds of Privacy Policies*, HEALTH CARE BLOG (Feb 22, 2016), http://thehealthcareblog.com/blog/2016/02/22/apple-and-the-3-kinds-of-privacy-policies [https://perma.cc/ZVJ5-27G8].

220. *See generally* Brian Barrett, *The Apple-FBI Battle Is Over, But The New Crypto Wars Have Just Begun*, WIRED (March 30, 2016), http://www.wired.com/2016/03/apple-fbi-battle-crypto-wars-just-begun/ [https://perma.cc/2F8A-RN8B]; Kim Zetter, *Apple's FBI Battle Is Complicated. Here's What's Really Going On*, WIRED (Feb. 18, 2016), http://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/ [https://perma.cc/CYF9-L2LB].

221. *See generally iOS Security: iOS 9.0 or Later*, APPLE, INC. (Sept. 2015), https://www.apple.com/business/docs/iOS_Security_Guide.pdf [https://perma.cc/9VVE-DZ2U].

222. *Transforming Health Care: The President's Health Information Technology Plan*, WHITE HOUSE: PRESIDENT GEORGE W. BUSH (Jan. 20, 2004), http://georgewbush-

solos for their file room predecessors. Thus, that 10-year plan rotated around the implementation of *interoperable* records. However, by 2009 "information systems in more than 90% of U.S. hospitals [did] not even meet the requirement for a basic electronic-records system."[223] Not surprisingly, therefore, the federal government's Meaningful Use subsidy program,[224] introduced by the HITECH Act, made interoperability a major goal,[225] albeit one that has proven particularly difficult to execute.[226]

The search for the magic bullet that will make clinical data more liquid within professional health-care space has implicated HIPAA privacy rules. Specifically, there are concerns that rigorous downstream data protection models impede data sharing. For example, a 2015 ONC report found that "privacy and security laws are cited in circumstances in which they do not in fact impose restrictions" such as when "providers . . . cite the HIPAA Privacy Rule as a reason for denying the exchange of electronic protected health information for treatment purposes, when the Rule specifically permits such disclosures."[227]

In its interoperability roadmap, ONC has laid out a ten-year plan for converting U.S. health care into a truly interoperable learning[228] health-care system.[229] Throughout, the report stresses that data protection will not suffer: "It is essential to maintain public trust that health information is safe and secure. To better establish and maintain that trust, stakeholders will strive to ensure that appropriate, strong and effective safeguards for electronic health information are in place as interoperability increases across the industry."[230]

Interestingly, the report also calls on stakeholders to "support greater

---

whitehouse.archives.gov/infocus/technology/economic_policy200404/chap3.html [https://perma.cc/2U68-DXS9].

223. Ashish K. Jha et al., *Use of Electronic Health Records in U.S. Hospitals*, 360 NEW ENG. J. MED. 1628, 1634 (2009).

224. *Electronic Health Records (EHR) Incentive Programs*, CTRS. FOR MEDICARE & MEDICAID SERVS., https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html [https://perma.cc/VVK8-82GJ].

225. *See* Deth Sao et al., *Interoperable Electronic Health Care Record: A Case for Adoption of a National Standard to Stem the Ongoing Health Care Crisis*, 34 J. LEGAL MED. 55 (2013).

226. *See* Terry, *supra* note 61, at 164–68.

227. Office of the Nat'l Coordinator for Health Info. Tech., *Report on Health Information Blocking*, U.S. DEP'T HEALTH & HUM. SERVS. 16 (Apr. 2015), https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf [https://perma.cc/3JNE-HUPT] [hereinafter *Report on Health Information Blocking*].

228. *See generally The Learning Healthcare System: Workshop Summary*, INST. MED. (LeighAnne Olsen et al. eds. 2007) https://www.nap.edu/catalog/11903/the-learning-healthcare-system-workshop-summary-iom-roundtable-on-evidence [https://perma.cc/5JVB-SCYL].

229. Office of the Nat'l Coordinator for Health Info. Tech., *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap*, U.S. DEP'T HEALTH & HUM. SERVS. (Oct. 2015), https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf [https://perma.cc/34M4-6AA2].

230. *Id.* at xiv.

transparency for individuals regarding the business practices of entities that use their data, particularly those that are not covered by the HIPAA Privacy and Security Rules, while considering the preferences of individuals."[231] This statement reads as a somewhat dejected admission that a dysfunctional regulatory system increasingly is hopeful of leveraging corporate stakeholder empathy to influence those they do business with to respect health-care data protection.

Due to the pressure to increase data interoperability and exchange, policymakers will continue to embrace calls to reduce some of the exceptional protections granted health-care data. The most likely initial casualty is the additional exceptional protections currently granted behavioral health records.[232] Although SAMSHA delivered on its promise to deliver an updated draft regulation within the next eighteen months,[233] its Congressional critics remain unimpressed.[234]

In the next few years, the increasingly difficult task for policymakers will be to distinguish between: first, the "noise" of overstating HIPAA barriers, second, attempts to use the goal of enhanced interoperability as a straw man designed to increase commercial expropriation of clinical data and third, genuine, nuanced policy collisions that require resolution (including data protection deprecation).

B. Medical and Population Health Research

Claims on clinical and medically inflected and health-determining data for research purposes are also increasing. Much of the research is taking place within clinical spaces. Of particular relevance to issues of data regulation, health-care providers claim that the growing field of outcomes research is covered by HIPAA's permitted use exception for "health care operations"[235] Other research involves big data analytics (examples include the President's *Precision Medicine Initiative*[236] and the NIH's Big Data to Knowledge program[237]) and typically uses de-identified clinical data or an identified "limited data set" subject to a data use

231. *Id.*

232. *See supra* text accompanying note 150 *et seq.*

233. *See supra* text accompanying note 150.

234. "This regulations [sic] continues the redundant multiple-step process that makes it a huge burden for patients, providers, and health care professionals that could make it difficult for a provider to get relevant information quickly and it is a barrier to integrated care." David Pittman, *Senate HELP Alters Its Health IT Draft*, POLITICO (Feb. 8, 2016), http://www.politico.com/tipsheets/morning-ehealth/2016/02/senate-help-alters-its-health-it-draft-212591 [https://perma.cc/8J9V-TYL5] (quoting email from office of Rep. Murphy).

235. 45 C.F.R. § 164.506 (2016).

236. *The Precision Medicine Initiative*, WHITE HOUSE, https://www.whitehouse.gov/precision-medicine [https://perma.cc/BE9M-RVM7].

237. *About BD2K*, NAT'L INST. HEALTH, https://datascience.nih.gov/bd2k/about [https://perma.cc/M8EW-6W8K].

agreement.[238] As noted by Barbara Evans, "[a] major challenge in twenty-first century privacy law and research ethics will be to come to terms with the inherently collective nature of knowledge generation in a world where large-scale informational research is set to play a more prominent role."[239] Jane Bambauer goes further, arguing that, because HIPAA "attempt[s] to anticipate and account for every public policy override, and set an otherwise inflexible rule of nondisclosure[,]" its "privacy provisions have had perverse effects on access to critical research data, quality of care, and overall public health."[240]

That tension between data protection and responsible research will only increase. Furthermore, technology continually chisels away at the professional-consumer health-care space divide. For example, the IOM has recommended that some social and economic determinants of health should be recorded in EHRs,[241] adding social media to clinical data shows promise,[242] and, increasingly, clinical research is occurring outside of recognized professional spaces using crowdsourcing or mobile apps such as those built around Apple's ResearchKit.[243]

C. Refuting the Binary

Arguments about the negative impact of data protection on clinical interoperability, medical research, or positive disruption suffer from one consistent shortcoming. They tend to posit unsupportable, simplistic binaries, painting "privacy" as oppositional to innovation or progress. There are several flaws underpinning this "all or nothing" position.

First, data protection rules that impact research or other data sharing, while occasionally deliberately obstructive, often are misinterpreted or used perversely to create barriers. In 2010 the President's Council of Advisors on Science and Technology noted how "The complex mandates of both HIPAA and state laws and regulations leads organizations to equate protection to sequestration, with little or no provision for either access based on roles . . . or for legitimate secondary uses of data . . . although HIPAA itself actually does allow disclosures in many such cases."[244] In the intervening years HHS-OCR, which is charged

238. 45 C.F.R. § 164.514 (2016).

239. Barbara J. Evans, *Much Ado About Data Ownership*, 25 HARV. J.L. & TECH. 69, 76 (2011).

240. Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 114 (2014).

241. Nancy E. Adler & William W. Stead, *Patients in Context — EHR Capture of Social and Behavioral Determinants of Health*, 372 NEW ENG. J. MED. 698 (2015).

242. *See, e.g.*, Kevin A. Padrez et al., *Linking Social Media and Medical Record Data: A Study of Adults Presenting to an Academic, Urban Emergency Dep't*, 25 BMJ QUALITY & SAFETY 414 (2016).

243. *See, e.g.*, Press Release, Apple, Inc., Apple Announces New ResearchKit Studies for Autism, Epilepsy & Melanoma (Oct. 15, 2015), http://www.apple.com/pr/library/2015/10/15Apple-Announces-New-ResearchKit-Studies-for-Autism-Epilepsy-Melanoma.html [https://perma.cc/6KG8-LBXF].

244. President's Council of Advisors on Sci. & Tech., *Report to the President Realizing the*

with HIPAA enforcement, has repeatedly issued guidance reminding stakeholders that HIPAA allows sharing of PHI between provider and patient[245] and between providers.[246] Equally, Congress[247] and ONC[248] have been critical of any attempts providers have made to use HIPAA as a barrier for intentional non-sharing, usually referred to as "information blocking." Ironically, medically-inflected data (the health-care data collected and processed outside of HIPAA protection) is likely more liquid than data held by traditional health-care providers. However, as technologies improve and both providers and patients become better educated about data sharing *within* a protected environment, that should change.

Second, data protection is contextual and the level of protection should be calibrated against particular data types, intended uses, and the commercial ambitions of data custodians. With regard to the last, and as noted by the FTC:

> Organizations have used big data to predict life expectancy, genetic predisposition to disease, likelihood of hospital readmission, and likelihood of adherence to a treatment plan in order to tailor medical treatment to an individual's characteristics. This, in turn, has helped health-care providers avoid one-size-fits-all treatments and lower overall health-care costs by reducing readmissions. Ultimately, data sets with richer and more complete data should allow medical practitioners more effectively to perform "precision medicine," an approach for disease treatment and prevention that considers individual variability in genes, environment, and lifestyle.[249]

In contrast, the commercial use of sensitive personal-health-care or medically-inflected data exported from or created outside of the health-care space impacts quite different policy questions. When data are being used by providers for, say, clinical outcomes research, restrictive rules are less called for so long as

---

Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward, EXECUTIVE OFFICE PRESIDENT 47 (Dec. 2010), https://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf [https://perma.cc/TCG3-TQQ7].

245. *See, e.g.*, *Individuals' Right under HIPAA to Access Their Health Information 45 CFR § 164.524*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html [https://perma.cc/KY6C-JMDU].

246. *Does the HIPAA Privacy Rule Permit a Doctor, Laboratory, or Other Health Care Provider to Share Patient Health Information for Treatment Purposes by Fax, E-mail, or Over the Phone?*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/faq/482/does-hipaa-permit-a-doctor-to-share-patient-information-for-treatment-over-the-phone/index.html [https://perma.cc/WTM9-75A2].

247. *See, e.g.*, 21st Century Cures Act, Pub. L. No. 114-255, § 4004, 130 Stat. 1033, 1176–80 (2016) (to be codified at 42 U.S.C. § 300jj-52).

248. *See, e.g.*, *Report on Health Information Blocking*, *supra* note 227, at 11–14.

249. *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues*, FED. TRADE COMMISSION 7 (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [https://perma.cc/WR4N-9AMB] [hereinafter *Big Data Report*] (references omitted).

the data are used for the stated purpose and kept within the clinical domain.

Third, "privacy" is not a single concept but rather is descriptive of a broad array of upstream and downstream protective models. Take a recent opinion piece by David Agus, which at first sight seemed to be adopting the anti-HIPAA rhetoric of medical research trumping privacy when he argued: "Patients understandably don't want their acquaintances and employers to know all their private health information. But we cannot let these fears suppress the powerful insights medical data can offer us."[250] Yet, elsewhere in the piece, he argued for increased data encryption and other security, careful protection against health-care data-driven discrimination and generally seemed to be arguing for the sharing of de-identified information.

The trick is that we can have both research and data protection. Similarly, data market disruption or mobile health disruption can drive progress in health care without exposing patient's data to exploitation. Neither need endanger properly calibrated health-care data protection.

VI. REGULATORY RESPONSES TO DISRUPTION AND ARBITRAGE

In the face of regulatory disruption and arbitrage, it should be no surprise that additional data protection is required to safeguard health-care information that resides outside of traditional, highly regulated spaces. Policymakers must address considerations of timing and approach together with the question of whether they need to add additional protections to continue the tradition of exceptionalism. First, however, it is worth considering whether to deal with the issue by attacking disruption, rather than by better regulating the disrupted state.

A. Is Disruption Worth the Trouble?

Is it possible to put a positive spin on disruption? Returning once again to the analogy of mobile health and ride-hailing apps, there seems little doubt that the traditional taxi industry presents with serious anti-competitive properties: a guild mentality, non-market limitations on the number of market participants via medallions, and agency capture to name just a few.[251] Is there an argument to be made that regulatory disruption does what policymakers often fail to do; to take a clean-sheet look at the regulation of innovative businesses rather than simply

250. David B. Agus, *Give Up Your Data to Cure Disease*, N.Y. TIMES (Feb. 6, 2016), http://www.nytimes.com/2016/02/07/opinion/sunday/give-up-your-data-to-cure-disease.html [https://perma.cc/KZ9M-YW4J]

251. *See generally* Rohin Dhar, *The Tyranny of the Taxi Medallions*, PRICECONOMICS (Apr. 10, 2013), http://blog.priceonomics.com/post/47636506327/the-tyranny-of-the-taxi-medallions [https://perma.cc/39FZ-UR9E]; Jason Snead, *Taxicab Medallion Systems: Time for a Change*, HERITAGE FOUND. (Dec. 10, 2015), http://www.heritage.org/research/reports/2015/12/taxicab-medallion-systems-time-for-a-change [https://perma.cc/8XJM-XHE3].

apply or add to the sedimentary layers of outdated laws?

Of course, health care makes the taxi industry look like a candidate for a Nobel Prize in economics. Indeed, there is nothing novel about the observation that health care fails to obey most market norms.[252] Equally, it is well known that at various times physicians, hospital administrators,[253] and insurers[254] have held market-controlling positions. Examples are legion and regulators, such as the FTC, do rail against some of the worst market abuses. For example, in *North Carolina State Bd. of Dental Examiners v. F.T.C.*, Justice Kennedy denied application of state antitrust immunity when government "abandon[s] markets to the unsupervised control of active market participants, whether trade associations or hybrid agencies."[255]

For every attempt to limit, say, guild power, there are defeats elsewhere, however. For instance, the Federal Trade Commission and the Antitrust Division of the U.S. Department have been sharply critical of health care's "medallion" systems such as state requirements for Certificates of Need (CON): "CON laws raise considerable competitive concerns and generally do not appear to have achieved their intended benefits for health care consumers. For these reasons, the Agencies historically have suggested that states consider repeal or retrenchment of their CON laws."[256] Yet, most courts seem unimpressed by legal challenges to these relics of 1970s centralized planning.[257]

Are, therefore, big data and mobile health disruptions positives? After all, entrenched stakeholders (incumbents) seem to have little interest in positively reforming data protection regimes. This is not always because of a genuine commitment to patient privacy. Rather, health-care stakeholders frequently view patient data as proprietary and will use the excuse of privacy to keep such valuable assets close. "Disruption as laboratory" is also a tempting model because of the current tension between data protection and data liquidity. In the words of Cisco executive Shanti Gidwani, "Disruptive is a good thing. . . It moves us to be transformational and innovative."[258]

---

252. Kenneth J. Arrow, *Uncertainty and the Welfare Economics of Medical Care*, 53 AM. ECON. REV. 941 (1963).

253. *See, e.g.*, PAUL STARR, THE SOCIAL TRANSFORMATION OF AMERICAN MEDICINE (1982).

254. *See, e.g.*, CHRISTY FORD CHAPIN, ENSURING AMERICA'S HEALTH, THE PUBLIC CREATION OF THE CORPORATE HEALTH CARE SYSTEM (2015).

255. 135 S. Ct. 1101, 1117 (2015).

256. Fed. Trade Comm'n & U.S. Dep't of Justice, Joint Statement of the Federal Trade Commission and the Antitrust Division of the U.S. Department of Justice on Certificate-of-Need Laws and South Carolina House Bill 3250, at 17 (Jan. 11, 2016), https://www.ftc.gov/policy/policy-actions/advocacy-filings/2016/01/joint-statement-federal-trade-commission-antitrust [https://perma.cc/22HR-R92Z].

257. *See, e.g.*, Colon Health Centers of Am., LLC v. Hazel, 813 F.3d 145 (4th Cir. 2016).

258. Jeremy Hainsworth, *Disruptive Techs Can Help Health-Care*, BNA NEWS (Feb. 17, 2016), http://www.bna.com/disruptive-techs-help-n57982067427 [https://perma.cc/W7QU-PU2T].

B. A Different Type of Laboratory, the States

With federal law allowing disruption and arbitrage and the absence of any clear legislative or regulatory paths, might state law fulfill its traditional laboratory role by implementing some stopgap measures? Clearly, states *do* operate in this space, although they may not conceptualize their actions as data protection. Take, for example, the impact of past criminal records on employment decisions. Federal law, represented by EEOC Guidance, takes the position that the overrepresentation of persons of color in "contact with the criminal justice system" could impact some discriminatory hiring or other employment decisions.[259] In contrast, several states have taken a far more direct approach, enacting "second chance" laws that permit convicted persons to withhold information about expunged crimes.[260]

In the health-care data protection space, few states have moved far from the HIPAA norm. Even California's Confidentiality of Medical Information Act,[261] long held out as the model for regulation that goes beyond HIPAA, does little to deal with the disruption and arbitrage discussed here. At first sight, the statute's inclusion of "[a]ny business that offers software or hardware to consumers shall be deemed to be a provider of health care"[262] suggests the obvious. However, additional verbiage and a cross-reference suggest that in reality regulatory coverage is only extended to some PHRs.

Texas goes further, more successfully increasing the scope of health-care data protection (albeit still concentrating on downstream models). For example, the Texas statute uses a far broader definition of "covered entity" than HIPAA to include a "business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or person who maintains an Internet site[.]"[263] The statute also prohibits unconsented to reidentification[264] and the sale of PHI.[265]

The "laboratory of the states" argument is always attractive during a time of Congressional logjam. Stakeholders are paying careful attention to forthcoming state privacy legislation, although for now there is little in the way of health-care data protection. For example, the Tenth Amendment Center and the ACLU

259. *See Consideration of Arrest and Conviction Records in Employment Decisions Under Title VII of the Civil Rights Act of 1964*, U.S. EQUAL EMP. OPPORTUNITY COMMISSION, https://www.eeoc.gov/laws/guidance/upload/arrest_conviction.pdf [https://perma.cc/3B6E-8HEU].

260. *See, e.g.*, Greg Glod, *"Second Chance" Legislation is Smart Criminal Justice Reform*, RIGHT ON CRIME (Apr. 10, 2015), http://rightoncrime.com/2015/04/second-chance-legislation-is-smart-criminal-justice-reform [https://perma.cc/W5ZG-G6HE].

261. CAL. CIV. CODE D. 1, Pt. 2.6 (West 2016).

262. CAL. CIV. CODE § 56.06(b) (West 2016).

263. TEX. HEALTH & SAFETY CODE ANN. § 181.001(a)(2) (West 2015).

264. TEX. HEALTH & SAFETY CODE ANN. § 181.151 (West 2015).

265. TEX. HEALTH & SAFETY CODE ANN. § 181.153 (West 2015).

recently participated in the coordinated announcement of various state data protection measures, primarily aimed at reducing surveillance.[266]

C. What Style of Regulation is Appropriate for Disruptive Technologies?

Nathan Cortez has offered a thoughtful critique of the conventional wisdom as to how agencies should regulate disruptive businesses.[267] His starting point is Tim Wu's context-based defense of "agency threats," sub-regulatory signals that include "statements of best practices, interpretative guides, private warning letters, and press releases" [268] directed at industries facing uncertainty or disruption.[269]

Threats are not intended as a permanent solution, but rather as part of a longer process. If successful and widely respected, it is possible that a threat may create an industry norm, removing the need for rulemaking at all. Alternatively, a threat regime may be a pilot, as it were, for eventual lawmaking. The law created by rulemaking or adjudication will then benefit from the facts developed under the threat regime.[270]

Cortez's opposing argument is that "agencies need not be so deliberate and tentative with regulating innovations—even disruptive ones."[271] Rather "[t]he public interest demands that agencies maintain their fortitude in the face of regulatory disruption. And, somewhat counterintuitively, new technologies can benefit from decisive, well-timed regulation."[272] Cortez argues, "[t]he trick is to craft enduring policy under high uncertainty[,]" suggesting the use of "sunsets" and "deadlines."[273]

An early sign of regulatory disruption in the mobile health space came with regard to patient safety when, in 2013, the FDA essentially ceded its regulatory territory with a sub-regulatory Guidance as to which mobile apps it would choose to regulate under Section 201(h) of the Federal Food, Drug, and Cosmetic Act.[274]

---

266. Mike Maharrey, *16 States Simultaneously Announce Efforts to Protect Privacy, #TakeCTRL*, TENTH AMEND. CTR. (Jan. 20, 2016), http://tenthamendmentcenter.com/2016/01/20/16-states-simultaneously-announce-efforts-to-protect-privacy/ [https://perma.cc/SNZ6-J5MX]; *see generally* Andy Greenberg, *5 Things Congress Should Learn From New State Privacy Bills*, WIRED (Jan, 21, 2016), http://www.wired.com/2016/01/five-things-new-state-privacy-bills-could-teach-congress/ [https://perma.cc/G7CE-NX7J]; Hamza Shaban, *To Strengthen Consumer Privacy, the ACLU Looks to the States*, BUZZFEED NEWS (Jan. 20, 2016), http://www.buzzfeed.com/hamzashaban/aclu-takes-consumer-privacy-battle-to-the-states#.luoj0nXMY [https://perma.cc/78AH-A22W].

267. Nathan Cortez, *Regulating Disruptive Innovation*, 29 BERKELEY TECH. L.J. 175 (2014).

268. Tim Wu, *Agency Threats*, 60 DUKE L.J. 1841, 1841 (2011).

269. *Id.* at 1848.

270. *Id.* at 1851.

271. Cortez, *supra* note 267, at 227.

272. *Id.* at 179–80.

273. *Id.* at 217.

274. *Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff*, U.S. FOOD & DRUG ADMIN., (Feb. 2015),

Under this Guidance, FDA elected to exercise regulatory discretion over common health related apps such as trackers.

Rather than solve problems, the guidance seems to have had the opposite effect, arguably supporting Cortez's arguments. For example, Apple omitted health-monitoring features such as blood pressure and stress level when it launched Apple Watch in 2015. It is widely believed that this decision was made, at least in part, because of regulatory concerns.[275] Subsequently, Apple CEO Tim Cook stated:

> We don't want to put the watch through the Food and Drug Administration (FDA) process. I wouldn't mind putting something adjacent to the watch through it, but not the watch, because it would hold us back from innovating too much, the cycles are too long. But you can begin to envision other things that might be adjacent to it -- maybe an app, maybe something else.[276]

In fact, FDA practice suggests a very light regulatory hand, featuring not only sub-regulatory guidance, but also under-enforcement. For example, so far the agency has only reined in one mobile app developer.[277]

Not surprisingly, developers are selling apps that apparently perform medical device functions, yet are "saved" from regulation by "small print" characterizations. For example, take the app "Instant Blood Pressure." Its developer includes the following in its FAQ:

> Instant blood pressure is not a medical device. It is for recreational use only. It is not a replacement for a medical grade blood pressure monitor. It is not intended for use in and should not be used for the diagnosis of disease or other conditions, or in the cure, mitigation, treatment or prevention of disease.[278]

As a matter of law, this statement is not determinative, as the manufacturer's

---

http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf [https://perma.cc/4FVZ-F6D7] (the Guidance is primarily the same as that originally issued in September 2013).

275. Daisuke Wakabayashi, *What Exactly Is an Apple Watch For?*, WALL ST. J. (Feb. 16, 2015), http://www.wsj.com/articles/challenge-of-apple-watch-defining-its-purpose-1424133615?mod=e2fb [https://perma.cc/3GQL-EMBK].

276. Allister Heath, *Apple's Tim Cook Declares the End of the PC and Hints at New Medical Product*, TELEGRAPH (Nov. 10, 2015), http://www.telegraph.co.uk/technology/apple/11984806/Apples-Tim-Cook-declares-the-end-of-the-PC-and-hints-at-new-medical-product.html [https://perma.cc/DJ4Y-6Q4U].

277. Letter from Food & Drug Admin. to Myshkin Ingawale, Biosense Technologies Private Limited, http://www.fda.gov/MedicalDevices/ResourcesforYou/Industry/ucm353513.htm [https://perma.cc/C9FQ-7N6S].

278. *Support FAQs*, INSTANT BLOOD PRESSURE, http://www.instantbloodpressure.com/support/ [https://perma.cc/CWA2-T97Z].

intent is objectively determined.[279] However, statements like this—and there are many similar statements included within other apps—at least temporarily allow for arbitrage as the app is characterized as consumer, rather than professional, in nature.

Regarding health-care data protection, HHS simply lacks regulatory authority over most of the mobile health activity. Very few mobile app developers or service providers will be covered entities or their business associates. Likely, even a guidance would be viewed as overreaching.[280] The furthest HHS-OCR has gone on its own has been to post a lightly-trafficked Q&A page for health app developers[281] and, as mentioned above, worked with the FTC and the FDA on a web-based interactive tool for app developers.[282] Under pressure from Congress, HHS (with a little help from the FTC) has made clear their relative powerless in the emerging mobile health space.

Health information is increasingly collected, shared, or used by new types of organizations beyond the traditional health care organizations currently covered by HIPAA, such as peer health communities, online health management tools, and websites used to generate information for research, any of which might be accessed on computers or smart phones and other mobile devices. If they are not determined to be health plans, health care clearinghouses, or health care providers conducting certain electronic transactions, and they are not acting on behalf of, or providing a service to, a HIPAA covered entity, they are not subject to the HIPAA standards for covered entities and business associates.[283]

Specifically, HHS's analysis pointed to five classes of data protection responsibilities in which non-covered entities faced lower data protection duties than HIPAA covered entities: access rights, third-party data use, security standards, required privacy notices, and disclosure limitations.[284]

The FDA has gingerly entered the data protection space with a series of sub-regulatory guidances on device security.[285] In a recent draft guidance, FDA

279. 21 C.F.R. § 801.4 (2016).

280. Consider the stakeholder concerns about ONC overstepping its authority in the 2016 NPRM on EHR certification. *See* Rajiv Leventhal, *ONC's New Leader Defends Agency's Role in EHR Oversight*, HEALTHCARE INFORMATICS (Sept. 20, 2016), http://www.healthcare-informatics.com/article/ehr/onc-s-new-leader-defends-agency-s-role-ehr-oversight [https://perma.cc/D2Q4-S4Y2].

281. *Health App Developers: Questions About HIPAA?*, U.S. DEP'T HEALTH & HUMAN SERVS., http://hipaaqsportal.hhs.gov/a/home [https://perma.cc/7UKQ-VHQQ].

282. *Mobile Health Apps Interactive Tool*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool [https://perma.cc/D9HK-E73S].

283. *Health Data Collected by Entities Not Regulated by HIPAA*, *supra* note 205, at 4.

284. *Id.* at 20–30.

285. *Guidance for Industry and FDA Staff: Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices*, U.S. FOOD & DRUG ADMIN., (May 2005), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/

"emphasize[d] that manufacturers should monitor, identify and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices."[286] Presumably, however, even this guidance would not apply to mobile medical apps that are currently excluded from device regulation under the 2015 Guidance.[287]

In 2013, the FTC published a lower-level, sub-regulatory "guide," *Marketing Your Mobile App: Get It Right from the Start*, that urged transparency, truthfulness, consent, and data minimization:

> Under the law, you still have to take reasonable steps to keep sensitive data secure. One way to make that task easier: If you don't have a specific need for the information, don't collect it in the first place. The wisest policy is to:
>
> 1. collect only the data you need;
> 2. secure the data you keep by taking reasonable precautions against well-known security risks;
> 3. limit access to a need-to-know basis; and
> 4. safely dispose of data you no longer need.[288]

Notwithstanding its lowly status, the agency has undoubtedly heightened the agency threat status of this "guide" through their subsequent agency enforcement activities with regard to security[289] and privacy.[290] Indeed, the FTC's track record in security cases warranted the publication of yet another guide in 2015, *Start*

---

ucm089593.pdf [https://perma.cc/8XW7-65J9]; *Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf* (OTS) Software, U.S. FOOD & DRUG ADMIN., (Jan. 2005), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf [https://perma.cc/N278-M3QK].

286. *Draft Guidance for Industry and Food and Drug Administration Staff: Postmarket Management of Cybersecurity in Medical Devices*, U.S. FOOD & DRUG ADMIN. 4 (Jan. 2016), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf [https://perma.cc/J382-SBP7].

287. *See supra* text accompanying note 274.

288. *Marketing Your Mobile App: Get It Right from the Start*, FED. TRADE COMMISSION 5 (Apr. 2013), https://www.ftc.gov/system/files/documents/plain-language/pdf-0140_marketing-your-mobile-app.pdf [https://perma.cc/WEM8-24WY].

289. *See, e.g.*, Fed. Trade Comm'n v. Wyndham Worldwide Corp., No. 14-3514 (3rd Cir. filed Aug. 24, 2015), http://www2.ca3.uscourts.gov/opinarch/143514p.pdf [https://perma.cc/A89H-VN29]; *see also* Press Release, Fed. Trade Comm'n, Fandango, Credit Karma Settle FTC Charges That They Deceived Consumers by Failing to Securely Transmit Sensitive Personal Information (Mar. 28, 2014), https://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers [https://perma.cc/5RL2-XFKX].

290. *See, e.g.*, Nomi Technologies, Inc., FTC No. 132-3251 (2015), https://www.ftc.gov/enforcement/cases-proceedings/132-3251/nomi-technologies-inc-matter [https://perma.cc/F8YW-EGQX].

with Security, A Guide for Business that is subtitled *Lessons Learned from FTC Cases*.[291]

In 2016 The FTC began hosting a "Mobile Health Apps Interactive Tool" jointly produced with HHS, ONC, and FDA designed to "give [mobile app developers] a snapshot of a few important laws and regulations from three federal agencies."[292] The FTC also has continued in its somewhat lonely role of curbing the worst excesses of big data. Recently it followed up on its 2014 *Data Brokers* report[293] with another report, *Big Data: A Tool for Inclusion or Exclusion?*[294] While the former was investigatory, the latter is a clear agency "threat," as the agency notes its specific (e.g., FCRA) and general (§5(a)) powers to police big data.

D. The Level of Regulation: The Case for Continued Exceptionalism

There seem to be few arguments that health-care data are not sensitive and deserving of protection. The real question in today's environment, is whether health privacy advocates should throw in their lot with those arguing for heightened protection across all domains. This section asks whether continuing calls for health data protection exceptionalism have any particular salience. Several claims seem to have merit.

First, from earliest times the physician-patient-data relationship has involved special data obligations. A patient holds health information (either literally or as data that can be released during diagnosis). The patient's rights over this data are protected by both ethical and legal principles; an autonomy model requiring consent to data sharing.[295] Thus, in both the legal and ethical senses, the patient (instrumentally) exercises this right of privacy when the patient gives a physician access to these data. In exchange for that consent the physician agrees to hold the data in confidence, an obligation sourced in ethical frameworks, the confidence tort, and ethical-legal hybrids such as the duty owed by fiduciaries.[296] In the

---

291. *Start with Security: A Guide for Business*, FED. TRADE COMMISSION (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [https://perma.cc/V3MG-V97W].

292. *Mobile Health Apps Interactive Tool*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool [https://perma.cc/S26G-T68P].

293. *Data Brokers*, *supra* note 3.

294. *Big Data Report*, *supra* note 249.

295. "The primary justification seems closer to respect for autonomy. . . . We owe respect in the sense of deference to persons' autonomous wishes not to be observed, touched, intruded on, and the like. The right to authorize or decline access is basic." BEAUCHAMP & CHILDRESS, *supra* note 36, at 313–14.

296. *See generally* Nicolas P. Terry, *What's Wrong with Health Privacy?*, 5 J. HEALTH & BIOMEDICAL L. 1, 1–32 (2009); *see also* SANDRA PETRONIO, BOUNDARIES OF PRIVACY: DIALECTICS OF DISCLOSURE 28 (2002) (describing operation of "communication privacy management" such that "when a person confides, the recipient is held responsible for the information and a set of expectations is communicated by the discloser.").

words of Bill Gardner:

> [H]ealth services data are the residue of the touches of living persons against the health care system. As such, they reflect the experience of those patients, even if such effects are often obscure to the analyst. The data are lit from within by the experience of patients, even if only faintly. Medical data are the relics of human suffering, recovery, and death. We wouldn't be looking at them if there wasn't a signal there.[297]

In the health-care domain, therefore, there is a deep, culturally significant, and relationship-based demand for the strongest level of data protection. As noted by the HITPC in 2010, "[t[he relationship between the patient and his or her healthcare provider is the foundation for trust in health information exchange, particularly with respect to protecting the confidentiality of personal health information."[298]

Second, patients have been conditioned to disclose all data to their health-care providers on the basis of this very promise; that such data will be protected like no other. This somewhat reductionist argument should not be dismissed lightly. Patients have grown up with a system that has seemed impervious to even basic data sharing. Almost every visit to a provider involves filling out a new intake form or, at least, updating insurance and other personal information. As had been argued, "[p]atients should not be surprised about or harmed by collections, uses, or disclosures of their information."[299] For the past 15 years almost every health-care encounter will have been marked by the production of a HIPAA privacy notice,[300] the right to inspect and obtain copies,[301] and receive an accounting of disclosures.[302] Think of the surprise, the dashed expectations if a patient was to find that his or her data no longer was exceptionally protected because of an informational accident as to where they were created (e.g., on a smartphone) or who was their curator (a data broker).

Third, health-care data deserves exceptional protection in the face of exceptional threats. Health-care data is a hot commodity on the dark web.[303] It is

297. Bill Gardner, *Ethics and Data: What's at Stake*, INCIDENTAL ECONOMIST (Sept. 25, 2015), http://theincidentaleconomist.com/wordpress/ethics-and-data-whats-at-stake [https://perma.cc/N68V-ZJU4].

298. Letter from Paul Tang, *supra* note 126.

299. *Id.*

300. 45 C.F.R. § 164.520 (2016).

301. 45 C.F.R. § 164.524 (2016).

302. 45 C.F.R. § 164.528 (2016).

303. *See generally* Damon Beres, *What You Should Know About the 'Dark Web,' An Anonymous Haven for Hackers*, HUFFINGTON POST (Aug. 19, 2015), http://www.huffingtonpost.com/entry/what-is-the-dark-web_55d48c50e4b0ab468d9f17d7 [https://perma.cc/6XZH-W8UC]; *see also* Andrea Peterson, *Why Hackers Are Going After Health-care Providers*, WASH. POST. (Mar. 28, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/why-hackers-are-going-after-health-care-providers [https://perma.cc/C2B5-R8YC].

the fastest growing target for cyber-attacks,[304] accounting for 21% of data breaches globally.[305] Data brokers see a strong market for health-based ratings products. App stores are populated by tens of thousands of health and wellness apps, often of dubious provenance. Even respectable outcomes and human subject researchers covet clinical data at a time when the choice architecture for patient consent has not been agreed upon.

Fourth, health-care data seems particularly susceptible to discriminatory and other harmful uses. As noted in the 2015 HITPC report, under U.S. law some "discriminatory uses of health information are either not prohibited or are expressly permitted (for example, use of health information in life and disability insurance decisions)."[306] The report also acknowledged, "a lack of consensus on which uses are 'harmful,' particularly with respect to health big data analytics, as well as an inability to predict which future uses could be harmful and which beneficial, creating challenges to enacting policies to prohibit or place additional constraints on such uses."[307] The real issue is that the use of health-care data outside of the clinical setting with the potential for real or perceived harms will devastate the trust that accompanied the initial patient sharing of data with the provider. Without trust, patients will share less, and both their clinical care and the responsible research that could be performed using those data will suffer.[308]

Finally, while as citizens we may generally view the market as the best available solution to our problems and support the liquidity of data to foster innovation, we continue to stake out some limits. Policymakers have spent untold energy in trying to reverse health care's chronic market failure[309] and make it work more like other "normal" products and services. But in the words of David Blumenthal, "[p]eople feel differently" about health care "than they do about the myriad other things that get bought and sold, without controversy, in normal markets."[310] And, as result "[g]overnment is involved in health care because

304. *See, e.g.*, Lucas Mearian, *Cyberattacks Will Compromise 1-in-3 Healthcare Records Next Year*, COMPUTERWORLD (Dec 8, 2015), http://www.computerworld.com/article/3013013/healthcare-it/cyberattacks-will-compromise-1-in-3-healthcare-records-next-year.html [https://perma.cc/6YP7-PS5Z]; Shannon Pettypiece, *Rising Cyber Attacks Costing Health System $6 Billion Annually*, BLOOMBERG (May 7, 2015), http://www.bloomberg.com/news/articles/2015-05-07/rising-cyber-attacks-costing-health-system-6-billion-annually [https://perma.cc/XV5L-4JZW].

305. *2015 First Half Review*, BREACH LEVEL INDEX 10 (Sept. 2015), http://www.breachlevelindex.com/pdf/Breach-Level-Index-Report-H12015.pdf [https://perma.cc/D73Q-3LVY].

306. *Health Big Data Recommendations*, *supra* note 158, at 12.

307. *Id.* at 12–13.

308. "Failing to pay attention to these issues undermines trust in health big data analytics, which could create obstacles to leveraging health big data to achieve gains in health and well-being." *Id.* at 13.

309. ARROW, *supra* note 252, at 941–73.

310. David Blumenthal, *What's the Big Deal About Drug Prices?*, COMMONWEALTH FUND BLOG (Oct. 9, 2015), http://www.commonwealthfund.org/publications/blog/2015/oct/whats-the-big-deal-about-drug-prices [https://perma.cc/LQ5E-NW6W].

Americans deeply desire the health care protections government provides."[311] In short, data protection regarding our health care *is* important enough to us to warrant exceptional protection.

VII. MOVING BEYOND HIPAA, EXPLORING THE POTENTIAL OF MULTIPLE DATA PROTECTION MODELS

Privacy policymakers and champions for regulation have pushed back against data brokers, accusing them of expropriation[312] and encouraging data determinism.[313] In many cases, the same accusations can be made against those collecting data with mobile apps (particularly those selling the data to big data brokers). In *The Black Box Society*, Frank Pasquale described how those data-gathering and analytic tools might impact health-care data subjects:

> [A] "body score" may someday be even more important than your credit score. Mobile medical apps and social networks offer powerful opportunities to find support, form communities, and address health issues. But they also offer unprecedented surveillance of health data, largely ungoverned by traditional health privacy laws (which focus on doctors, hospitals, and insurers). Furthermore, they open the door to frightening and manipulative uses of that data by ranking intermediaries— data scorers and brokers— and the businesses, employers, and government agencies they inform.[314]

In its 2014 report on data brokers' practices, the FTC noted how health information or medically-inflected data was used to create "potentially sensitive categories [that] highlight certain health-related topics or conditions, such as "Expectant Parent," "Diabetes Interest," and "Cholesterol Focus."[315] In *Here's Looking at You*, the California HealthCare Foundation noted:

> Consumer scores are now ubiquitous across peoples' activities: financial and credit, energy use, law enforcement, environmental, social clout, tax returns, environmental "green-ness," and health. In 2014, there were at least a dozen health scores available in the marketplace, including the

311. *Id.*

312. Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at the 23rd Computers, Freedom, and Privacy Conference: Reclaim Your Name 11–12 (June 26, 2013), http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf [https://perma.cc/Y4KU-FUN4].

313. Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Keynote Address at the Tech. Pol'y Inst. Aspen Forum: The Privacy Challenges of Big Data: A View from the Lifeguard's Chair 7 (Aug. 19, 2013), http://ftc.gov/speeches/ramirez/130819bigdataaspen.pdf [https://perma.cc/XS6V-BAVT].

314. FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 26 (2015) (references omitted).

315. *Data Brokers*, *supra* note 3, at 47.

> Affordable Care Act (ACA) Individual Health Risk Score, FICO Medication Adherence Score, several frailty scores, personal health scores (e.g., WebMD, One Health Score), and medical complexity scores (e.g., Aristotle for scoring of surgery for congenital health conditions). Consumers are largely unaware of the existence and use of these scores and the algorithms that create them.[316]

Notwithstanding its flaws, HIPAA was a reasonable approach to health-care data protection in the last decade of the twentieth century. At the time, both "privacy" and security threats primarily arose from inside the health-care system. Data protection required an update from the haphazard nature of state confidentiality-based protections as the industry swapped PCs for paper, while hospital IT needed a solid nudge to lock some doors and reduce the number of stolen laptops and thumb drives. As such, combining a solid, if exclusively downstream, national HIPAA floor and compliance-based policing made some sense.

Fast-forward to 2009, and policymakers seemed unable to look to the future. The HITECH Act was designed to improve the HIPAA system just enough to absorb the unprecedented growth of EHRs, which the same legislation was about to subsidize.[317] The only attempt to think outside the hospital-based technology box was the introduction of a breach notification rule for PHRs. Yet, the implications of big data mining and data aggregation were already being discussed and the iPhone's introduction in 2007,[318] followed a year later by its app store,[319] suggested the birth of a mobile revolution.

The closing argument of this article is that today the traditional, exceptional, justifiably high protection of health-care data is seriously threatened by the disruption and arbitrage displayed in big data and mobile spaces. Waiting in the wings are other threats from emerging, more autonomous technologies such as the Internet of Things, self-driving vehicles, and robots.[320]

Because of the threats to health-care data protection, legislation providing for data minimization and context-based limitations is urgently required.

---

316. *Here's Looking at You: How Personal Health Information Is Being Tracked and Used*, CAL. HEALTH CARE FOUND., 8 (July 2014), http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/PDF%20H/PDF%20HeresLookingPersonalHealthInfo.pdf [https://perma.cc/L9TG-Y3XJ].

317. *See generally* Terry, *supra* note 108.

318. Press Release, Apple, Inc., Apple Reinvents the Phone with iPhone (Jan. 9, 2007), https://www.apple.com/pr/library/2007/01/09Apple-Reinvents-the-Phone-with-iPhone.html [https://perma.cc/73ZX-8BA5].

319. Michael Arrington, *iPhone App Store Has Launched (Updated)*, TECHCRUNCH (July 10, 2008), http://techcrunch.com/2008/07/10/app-store-launches-upgrade-itunes-now [https://perma.cc/FS55-W2RS].

320. *See, e.g.*, Drew Simshaw et al., *Regulating Healthcare Robots: Maximizing Opportunities While Minimizing Risks*, 22 RICH. J.L. & TECH. 3 (2016); Nicolas Terry, *Will the Internet of Things Disrupt Healthcare?*, 19 VAND. J. ENT. & TECH. L. ___ (forthcoming 2017).

Consider, for example, some features of the European General Data Protection Regulation[321] that maintain or even strengthen existing data protections that have existed under the EU Data Directive.[322] In this scenario, processing of "data concerning health" is prohibited unless it falls within quite limited exceptions including diagnosis and some research.[323] Further, the "purpose limitation" endures such that "Personal data shall be . . . collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."[324] Along with data minimization, the purpose limitation puts major constraints on big data collection and analytics.[325] The regulation also restricts the use of "automated processing, including profiling."[326]

The most appropriate solution would be for Congress to enact a new, hopefully FIPPS-rich, federal privacy code and/or give rule-making power to the FTC or some new data protection agency (perhaps a model based on Senator Elizabeth Warren's Consumer Financial Protection Bureau). Any code or regulations could apply equally to all data types. Or, as seems more likely, they could also single out certain sensitive data types such as health data for additional protection. Whichever route Congress were to adopt, they must apply the correct approach to any future "sectoral" model of protection. First, agree on the general protective principles, and only then build out conceptually consistent protections.

Framed in large part, although not exclusively, by the explosion of big data services, various branches of the federal government published privacy reports and proposals between 2012 and 2015. All favored increased regulation, including of data brokers, yet failed to agree on much else.[327] Thereafter, and with implications for mobile health, the FTC recommended broad,

---

321. *Supra*, discussion on page 252.

322. *See, e.g.*, Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281/42), § 6 http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046.

323. Commission Regulation 2016/679, art. 9, 2016 O.J. (L 119) 1, 38.

324. *Id.* art. 5.

325. *See generally* Opinion of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Article 29 WP, Opinion 03/2013 on Purpose Limitation, 00569/13/EN, WP 203 (April 2, 2013) at 45–47, Example 9, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [https://perma.cc/XDA6-VRL3].

326. Commission Regulation 2016/679, art. 22, 2016 O.J. (L 119) 1, 46.

327. *Framework for Protecting Privacy*, *supra* note 18; *Protecting Consumer Privacy*, *supra* note 40; *Big Data: Seizing Opportunities*, *supra* note 77; President's Council of Advisors on Sci. & Tech., *Big Data and Privacy: A Technological Perspective*, EXECUTIVE OFFICE PRESIDENT, (May 2014), http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [https://perma.cc/QN7C-CMXP]; *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015*, WHITE HOUSE (2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [https://perma.cc/57XV-3HYB].

technologically-neutral privacy legislation backed up with self-regulatory programs for the Internet of Things.[328]

There is no indication that these recommendations have any traction or that Congress would even consider such sweeping legislation. However, there is the potential—particularly in the wake of, say, some massive big data breach or scandal-quality privacy violation—that Congress might consider highly targeted legislation providing for explicit consent to health data being shared with data brokers. In its data brokers report, the FTC urged: "Congress should . . . consider imposing important protections for sensitive information, such as certain health information, by requiring that consumer-facing sources obtain consumers' affirmative express consent before collecting and sharing such information with data brokers."[329] Such baseline legislation likely would satisfy Cortez's "enduring policy" goal while other, more comprehensive proposals are explored through guidance and codes of conduct.

Another approach would be to extend HIPAA applicability to all custodians or processors of health-care data. Consider an analogous, superficially attractive, yet ultimately naïve, approach to health-care reform: Medicare for All, achieved by removing the age eligibility from federal coverage and, creating a single payer, universal care health-care system.[330] Yet, whether judged through political, constitutional, or organizational lenses, it isn't that simple. As Harold Pollack notes, "Medicare for All cannot offer itself as the replacement of our depressing health politics. It would have to arise as another product of that very same process, passing through the very same legislative choke points, constrained by the very same path dependencies that bedevil the ACA."[331]

Similarly, the answer to whether HIPAA should be broadened with a single stroke of the pen also must be "no." Such an extension of HIPAA is not rejected on normative grounds. Health-care data residing outside traditional health-care space should receive no less protection than that inside it. Indeed, a good argument can be made that the former deserves *more* legal protection because health-care insiders are additionally constrained or policed by professional standards and ethics thus reducing data subjects' privacy risks. HIPAA's approach to data protection is exclusively mapped to and calibrated for the traditional health-care domain. The existential threats to health-care data protection are from outside of the professional domain and they are not threats that can be countered only with downstream data protection models. HIPAA was

328. FED. TRADE COMMISSION, *supra* note 118, at 48–49.

329. *Data Brokers*, *supra* note 3, at 52.

330. Nancy Altman, *How and Why Medicare for All Is a Realistic Goal*, HUFFINGTON POST BLOG (Jan. 24, 2016), http://www.huffingtonpost.com/nancy-altman/how-and-why-medicare-for_b_9063970.html [https://perma.cc/JD42-C8SA].

331. Harold Pollack, *Medicare for All—If It Were Politically Possible—Would Necessarily Replicate the Defects of Our Current System*, 40 J. HEALTH POL., POL'Y & L. 921, 926 (2015).

specifically designed to map (whether successfully or not) to professional health-care workflows and issues. Any fundamental broadening of its scope would be highly problematic. Most importantly, the data protection problems highlighted by big data and mobile health suggest that upstream regulatory models are required, not the types of downstream protections (HIPAA privacy, security and breach notification) offered by HIPAA.

Given the problems associated with extending HIPAA and absent broad privacy legislation, what would be most effective in reducing or eliminating regulatory disruption and arbitrage in health-care data protection? In this admittedly imperfect world, this article suggests three strategies. First, HHS-OCR and the FTC should focus particular enforcement attention on the protection of HIPAA-zone data that are sources for big data. Second, ONC should use its existing regulatory powers to tighten up some aspects of the existing HIPAA privacy and security rules. Third, if politics continue to get in the way of comprehensive federal privacy legislation, Congress should at least pass narrower provisions aimed at some of the more obvious targets.

A. Increased Enforcement

Particularly with regard to big data brokers, both OCR and FTC need to remain vigilant and, through rigorous enforcement, pressure brokers to reform their practices to the benefit of consumers. There is little doubt that some HIPAA-zone data migrates into big data. Here, strong OCR enforcement of the existing data protection rules may deter some big data collection. For example, there should be heightened scrutiny of compliance with the requirements for PHI de-identification,[332] particularly with regard to the addressing of the potential for re-identification under HIPAA's "expert" (or statistical) method.[333] OCR should also dedicate particular enforcement attention to large caches of human subjects research data to ensure the highest levels of privacy and security for research subjects.[334]Additionally, OCR should extend its recent interest[335] regarding the

---

332. *See, supra*, text accompanying notes 90-91.

333. *See generally How Do Experts Assess the Risk of Identification of Information?*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/#idrisk [https://perma.cc/C7VC-TQTZ] (providing risk assessment information regarding the risk of reidentification of various identifiers).

334. *See, e.g.*, Corrective Action Plan between the United States Department of Health and Human Services and the Feinstein Institute for Medical Research (Mar. 16, 2016) ($3.9m settlement with research institute that had exposed the PHI of 13,000 individuals), http://www.hhs.gov/sites/default/files/FIMR%20Resolution%20Agreement%20and%20Corrective%20Action%20Plan.pdf [https://perma.cc/HLE3-4D58].

335. Corrective Action Plan between the United States Department of Health and Human Services and Raleigh Orthopaedic Clinic, P.A. (Apr. 14, 2016) ($750,000 settlement), http://www.hhs.gov/sites/default/files/Raleigh%20Orthopaedic%20RA%20%26%20CAP%20%28508%29_0.pdf [https://perma.cc/NZB5-5TWJ]; North Memorial Health Care Resolution Agreement and Corrective Action Plan, ($1.55m settlement),

formation of business associate agreements (BAAs)[336] to scrutinizing the contemplated use of PHI in BAAs.[337] Meanwhile, the FTC should continue to address point-of-use discriminatory and other unfair practices with both its general powers under the FTC Act and its specific authority under the Fair Credit Reporting Act and other equal opportunity laws, as it promised in its *Tool for Inclusion or Exclusion* report.[338]

B. Amendments to the Privacy and Security Rules

Business Associates aside, ONC lacks authority to regulate data custodians who are not covered entities.[339] Notwithstanding this limitation, the agency could tighten up the protection of PHI or data that has been protected as PHI. As a result, the HIPAA Privacy Rule should be amended to require:

Any de-identified data derived from patient clinical information should be subject to a data use agreement prohibiting re-identification.

The Security Rule should be amended to require:

PHI data must be encrypted both in motion and at rest.

These amendments would lessen the risk of unlawful "exports" of PHI. They would also require mobile apps produced by covered entities or their business associates to adopt high levels of data protection for consumer-facing apps that collect, process, or transfer PHI.[340]

C. Targeted Federal Legislation

As already noted the probability for even targeted federal legislation being considered by Congress is low. However, political bodies are reactive and if there

---

http://www.hhs.gov/sites/default/files/North%20Memorial%20RA%20and%20CAP%20March%202016%20%28508%29.pdf [https://perma.cc/85XQ-CN44].

336. *See* 45 C.F.R. § 160.103; 164.502(e), 164.504(e) (2016).

337. On a side note, providers should ensure that the BAAs they sign with big data providers do not allow data generated within the HIPAA zone to be exported for purposes not related to permitted uses. 45 C.F.R. § 164.501 (2016). On concerns about leakage from health-care systems as a result of such agreements, see Subhajit Basu, *Should the NHS share patient data with Google's DeepMind?* WIRED UK (May 16, 2016), http://www.wired.co.uk/article/nhs-deepmind-google-data-sharing [https://perma.cc/9BTE-CP4Q]; Ben Quinn, *Google Given Access to Healthcare Data of Up to 1.6 Million Patients*, GUARDIAN (May 4, 2016), https://www.theguardian.com/technology/2016/may/04/google-deepmind-access-healthcare-data-patients [https://perma.cc/E9YE-88DK].

338. *Big Data Report*, *supra* note 249.

339. See, *supra*, text accompanying note 85 *et seq*.

340. Non-HIPAA regulated apps would be subject to FTC ex post facto regulation if encryption was, for example, claimed but not implemented. *See* Press Release, Fed. Trade Comm'n, Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers by Failing to Securely Transmit Sensitive Personal Information (Mar. 28, 2014), https://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers [https://perma.cc/82S3-6ZY5].

was to be some major breach or some other high profile abuse of health information in the mobile or big data space there might be the opportunity for targeted legislation.

Any such legislation would face a threshold, definitional issue. Data protected by HIPAA is defined both by data type (PHI) and by custodian type (covered entity). Exceptional treatment of health data will require a new definition that is custodian-agnostic. The EU GDPR contains a usable definition: "'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."[341] Examples of limited, targeted legislation include the following:

Any "data concerning health" collected by non-HIPAA covered entities must only be used for the limited purpose for which it was collected.

Consumer-facing sources must obtain consumers' affirmative express consent before collecting and sharing "data concerning health" with data brokers.[342]

Point-of-use prohibitions for discriminatory uses of "data concerning health" must be expanded.

Data custodians are prohibited from re-identifying or attempting to re-identify any individual who was the subject of protected health information that has been de-identified.[343]

All custodians of "data concerning health" must provide access to the data upon request from any identified or identifiable data subject and implement systems enabling correction or deletion of such data.

As is evident, these suggested reforms (even if all were passed into legislation) fall well-short of any more utopian calls for comprehensive data protection legislation. However, each proposal is true to the spirit of FIPPS and, even if adopted singly, each would reduce the current disruption and arbitrage in health care data protection.

CONCLUSION

At the root of the arguments advanced in this article is one unassailable fact: vast quantities of health-care data are now being exported to, or created outside of, HIPAA-protected spaces. The upshot is a dramatically uneven policy environment. The holders of vast amounts of health-care-like data increasingly benefit from low or no data protection. Existing "protections" are being applied to similar data not on the basis of any rational distinctions, but on the basis of an

341. Commission Regulation 2016/679, art. 4(15), 2016 O.J. (L 119) 1, 34.

342. The FTC proposal from 2014, discussed *supra* note 329.

343. Based on the Texas provision, discussed *supra* notes 263–265.

accident of creation or current, possibly transient, states. Health-care professionals, patients, pre-patients, and responsible data processors all suffer mightily from this uneven policy environment.

There is little doubt that increasingly our "medical selves" will exist outside of the traditional, HIPAA-regulated health-care domain. As regulatory disruption and arbitrage increase, this will create progressively exploitable confusion as health information moves in and out of differentially protected domains. There is now massive commercial value to be extracted from health-care data, leading data aggregators and processors to perform an end-run around health care's domain-specific protections by creating medical profiles (HIPAA proxies) of individuals in HIPAA-free space. This will only increase as the possibilities of the Internet of Things, robotics, autonomous vehicles, and technologies not yet imagined interact with our medical selves.

Unfortunately, as Fleischer recognized, "[i]n the [last] twenty-five years . . . the administrative state has increased substantially, and the amount of time lawyers devote to regulatory matters has grown apace."[344] As a result, "[t]he complexity of the modern administrative state provides more opportunities for regulatory arbitrage--another form of value creation for the client--than ever before."[345] Further, as Brad Smith, Microsoft's Chief Legal Officer, recently noted in the context of the collapse of U.S.-EU safe harbor, "privacy rights cannot endure if they change every time the data moves from one location to another. Individuals should not lose their fundamental rights simply because their personal information crosses a border."[346] Or, in this case, move from a hospital EHR to an iPhone.

Some policymakers now recognize (albeit belatedly) that the protection of health-care data is diminished when it is created in or migrates to the HIPAA-free zone; a place of considerably reduced, even zero data protection. There has also been some recognition that this new state results in regulatory turbulence, disruption, and, at least in the case of big data, regulatory arbitrage. It is less clear whether policymakers recognize the multi-faceted nature of the problem. Although a downstream, compliance-based data protection model such as HIPAA can deal with a relatively cohesive domain, it is ill-prepared for the variety of challenges that occur when data are created outside of the that domain. As a result, merely extending the domain protection is unlikely to work well. Further, the dangers associated with a HIPAA-free zone are not limited to disruption because of uneven data protection domains, but are exacerbated by the

344. Fleischer, *supra* note 64, at 237.

345. *Id.*

346. Brad Smith, *The Collapse of the US-EU Safe Harbor: Solving the New Privacy Rubik's Cube*, MICROSOFT (Oct. 20, 2015), http://blogs.microsoft.com/on-the-issues/2015/10/20/the-collapse-of-the-us-eu-safe-harbor-solving-the-new-privacy-rubiks-cube/ [https://perma.cc/74XE-ZYBZ].

chronic weaknesses of the non-HIPAA data protection models.

In 2009, the HITECH Act instructed HHS and FTC to "conduct a study, and submit a report . . . on privacy and security requirements for entities that are not covered entities or business associates."[347] This was to be followed by the HHS Secretary reporting to Congress on "the findings of the study . . . includ[ing] in such report recommendations on the privacy and security requirements described in such paragraph."[348] ONC's 2016 "Examining Oversight" purports to be that report,[349] even though HHS officials described it as "the first step in a conversation,"[350] and it failed to discuss big data and other existential threats to health-care privacy, or present meaningful recommendations. Yet the need for granular, workable proposals for legislation, particularly FIPPS-infused upstream protections, has never been greater.

In the meantime, the exceptional protection of health data is being depreciated. There are many reasons and forces conspiring to make this happen. Some are decisions that go back to the U.S. "original sin" of eschewing a comprehensive privacy law of general applicability. Some are instrumental, including the competing forces for data, be they commercial big-data brokers or the National Institutes of Health. Some are historical, such as the traditional ways U.S. data protection has been structured—sectoral and downstream, characteristics that tend to create regulatory turbulence, even arbitrage. Some are technological, as we come to terms with new generations of personal connected devices and the vast power of cloud-based data storage and analysis. Whether at root, this is an issue of health-care-privacy exceptionalism or of the general inadequacy of data protection in the United States is somewhat moot. Whatever the causes, exceptional health data protection must be preserved and protected by increased enforcement and new regulation designed to not only curtail contemporary regulatory disruption and arbitrage, but also to proactively address the inevitable technologically-enabled threats that will follow.

347. HITECH Act § 13424(b)(1), 42 U.S.C. § 17953 (2012).

348. HITECH Act § 13424(b)(2).

349. *Health Data Collected by Entities Not Regulated by HIPAA*, *supra* note 205, at 1 n.4.

350. Karen B. DeSalvo & Jocelyn Samuels, *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA*, HEALTH IT BUZZ BLOG,. (July 19, 2016), https://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/examining-oversight-privacy-security-health-data-collected-entities-not-regulated-hipaa [https://perma.cc/4HDE-S7HE].